1503.68508 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re U.S. Patent Application )
)
Applicant: Tokutani et al. )
)
Serial No. )
)
Filed: October 6, 2003 )
)
For: PRIVATE DATA PROTECTION )
DISTRIBUTION METHOD )
AND PROGRAM )
)
Art Unit: )

*I hereby certify that this paper is being deposited with the United States Postal Service as EXPRESS MAIL in an envelope addressed to: Mail Stop PATENT APPLICATION, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this date.*

*Oct. 6, 2003* Daniel Canan
*Date* *Express Mail Label No.: EV032735215US*

**CLAIM FOR PRIORITY**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants claim foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

Japanese Patent Application No. 2002-296778, filed October 9, 2002

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By
Patrick G. Burns
Registration No. 29,367

October 6, 2003

300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
Telephone: 312.360.0080
Facsimile: 312.360.9315

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: October 9, 2002

Application Number: Patent Application No. 2002-296778
[ST.10/C]: [JP2002-296778]

Applicant(s): FUJITSU LIMITED

August 18, 2003

Commissioner,
Japan Patent Office Yasuo IMAI

Certificate No. P2003-3067294

1503.68508
312.360.0080

96

# 日本国特許庁
# JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１０月　９日

出願番号
Application Number: 特願２００２－２９６７７８

[ST. 10/C]: [ＪＰ２００２－２９６７７８]

出願人
Applicant(s): 富士通株式会社

２００３年　８月１８日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０６７２９４

【書類名】　特許願
【整理番号】　0251343
【提出日】　平成14年10月 9日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/00
【発明の名称】　個人データ保護流通方法及びプログラム
【請求項の数】　5
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　徳谷　崇
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　畠山　卓久
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　松永　宏
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100074099
【住所又は居所】　東京都千代田区二番町８番地２０　二番町ビル３Ｆ
【弁理士】
【氏名又は名称】　大菅　義之
【電話番号】　03-3238-0031

【選任した代理人】

【識別番号】　100067987

【住所又は居所】　神奈川県横浜市鶴見区北寺尾７－２５－２８－５０３

【弁理士】

【氏名又は名称】　久木元　彰

【電話番号】　045-573-3683

【手数料の表示】

【予納台帳番号】　012542

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705047

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　個人データ保護流通方法及びプログラム

【特許請求の範囲】

【請求項１】暗号化された個人データを受信するステップと、

暗号化された、該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを受信するステップと、

前記復号鍵と個人データ使用ライセンスを復号するステップと、

前記個人データの用途が前記個人データ使用ライセンスに記述された使用条件と一致するかを判断するステップと、

前記個人データの用途が前記使用条件と一致するときのみに前記復号された復号鍵を用いて前記個人データを復号するステップとを有することを特徴とする個人データ保護流通方法。

【請求項２】前記復号鍵と個人データ使用ライセンスはＤＲＭ認証技術を用いて暗号化及び復号化されることを特徴とする請求項１に記載の個人データ保護流通方法。

【請求項３】前記個人データ使用ライセンスをＤＲＭ認証技術を用いて復号化するための機構は、ＴＲＭ化されていることを特徴とする請求項２に記載の個人データ保護流通方法。

【請求項４】前記暗号化された個人データ及び該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを複数の情報主体より受信するステップと、

複数の前記個人データ使用ライセンスを同一な条件の単位で連結して名簿ライセンスを作成するステップと、

該名簿ライセンスの作成に使用された個人データ使用ライセンスに対応する、暗号化された個人データを連結して名簿を作成するステップを有することを特徴とする付記１に記載の個人データ保護流通方法。

【請求項５】暗号化された個人データを受信するステップと、

暗号化された、該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを受信するステップと、

前記復号鍵と個人データ使用ライセンスを復号するステップと、

前記個人データの用途が前記個人データ使用ライセンスに記述された使用条件と一致するかを判断するステップと、

前記個人データの用途が前記使用条件と一致するときのみに前記復号された復号鍵を用いて前記個人データを復号するステップとをコンピュータに実行させることを特徴とする個人データ保護流通プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

情報主体から個人情報を取得し、利用する個人情報取扱業者において、情報主体からその個人情報の使用を制限する個人データ保護流通システムに関する。

【０００２】

【従来の技術】

近年、プライバシーマーク制度、個人情報に関する様々な省庁から出されたガイドラインや個人情報保護法案また、Ｗ３Ｃで策定されているＰ３Ｐなど個人情報の取り扱いについて関心が集まっている。

【０００３】

Ｗ３Ｃ（World Wide Web Consortium）は、インターネット上で利用できるサービスの各種標準仕様を策定する目的で、１９９４年に米ＭＩＴコンピュータ・サイエンス研究所（Massachusetts Institute of Technology, Laboratory for Computer Science）に設立された非営利団体である。ＨＴＭＬやＸＭＬなど、様々なインターネット標準を策定している。また、Ｐ３Ｐ（Platform for Privacy Preferences）は、Webサイトのプライバシー・ポリシーを記述するための標準フォーマットである。Ｗ３Ｃによって現在標準化が進められている。これにより、ユーザ側のエージェント・ソフトウェアが、当該Webサイトのプライバシー・ポリシーを自動的に取得して解釈し、あらかじめユーザによって設定された個人情報の取扱基準に照らし合わせて、その挙動を切り替えられるようになる。

【０００４】

例えば、Webサイトまで要求しないまでも、Cookieを使用して、サイトをアクセスしているユーザを特定し、ユーザの挙動をモニタしていたりするところが少なくない。従来、こうしてWebサイト側が入手した個人情報が、どのようなポリシーに沿って運用されるかを確認するには、各サイトのプライバシー・ポリシーをユーザ自身が調査する必要があった。こうした処理をソフトウェアが自動的に行えるように、サイトのプライバシー・ポリシーを標準的なフォーマットで記述するために考案されたものがＰ３Ｐである。これにより、ユーザは、あらかじめWebブラウザなどで個人情報の取扱基準を設定しておき、Webサイトのプライバシー・ポリシーがこの基準に逸脱しないかどうかを自動的に判断できるようになる。

【０００５】

このように、Ｐ３Ｐは、アクセスしたWebサイトのプライバシー・ポリシーをソフトウェアが自動的に取得、解釈するための技術的なメカニズムを提供するが、記述されたポリシー通りにWebサイトが運営されるかどうかを保証するものではないので注意が必要である。また、Ｐ３Ｐ自体には、ユーザとWebサイトの間で個人情報を安全に転送する手段は規定されていない。データを安全に転送するためには、別の手段を講じる必要がある。

【０００６】

特に、米Harris　Interactive社の意識調査によると、個人情報に関する一般消費者の関心事の内、消費者の懸念事項のトップには「企業が無断で個人情報を他の企業と共有すること」が挙げられており、また企業が信頼に値するかを判断する上で重要視するトップ項目には、「顧客の個人情報を当人の許可無く、あるいは法律によって求められない限り開示しない」という事項が挙げられている。

【０００７】

したがって、個人が、安心して個人情報を提供するには、最低限個人情報の運用に関して二次使用の禁止や目的外使用の禁止、また、個人が自分の個人情報がどこでどのように使用されているかの把握と制御（情報主体のコントロール権）が重要であると考えられる。

【０００８】

また、各省庁のガイドラインや日本工業規格のＪＩＳ　Ｑ　１５００１、あるいは（２００２年４月）現在法律案ではあるが、個人情報保護法案などの様々なガイドラインや認定評価制度、法律においても上記３点に加え、事業者の個人データの安全管理、及び安全な収集について重要視している。

【０００９】

以上をまとめると、個人データを保護するためには、少なくとも以下の５つの要件を満足しなければならない。

（１）事業者は、情報主体に対して個人データの使用目的を告知し、その目的範囲内で使用しなければならない。（目的外の使用・不正使用の禁止）

（２）事業者は、不正に個人データを提供してはならない。（不正提供・二次使用の禁止）

（３）事業者は、個人データを安全に保管し、管理しなければならない。（安全な保管・管理）

（４）事業者は、個人データを安全に収集しなくてはならない。（安全な収集）

（５）事業者は、情報主体に対して、要求があった場合には、いつでもその情報主体の個人データを開示したり、訂正したり、削除しなければならない。（情報主体のコントロール権の確保）

従来では次のような対策を講じている。

（１）企業内で個人情報管理規定を定め、遵守する。

（２）（１）と同様、企業内で個人情報管理規定を定め、遵守する。たとえば、特定の従業員にしか個人データが保管しているデータベースへのアクセス権を与えないといったものがある。

（３）以下のような対策が採られている。

【００１０】

（ア）外部からアクセスできない場所におく。

（イ）個人データを暗号化などして保存する。

（ウ）パスワード認証によりアクセスしてくる個人の正当性を判断し、その後ロールベース（役職などに基づいて）のアクセス制御によりどのファイルにアクセスできるかを制御する。

【００１１】

（エ）だれが、どのようなアクセスをしたのかのログを記録する。

（オ）データのバックアップ。バックアップしたメディアなどをロッカーなどに鍵をかけて保管する。

（４）予め情報主体に同意を得た上で提供してもらう。そのとき、個人データは、暗号通信などを使って送られる。

（５）サイト上でアカウントを取得し、サイト上で自分の個人データを確認、訂正、削除などをできるようにする。

【００１２】

また、現在行われている個人情報を取り扱うサービスにおいて、センターが個人ユーザから個人データを収集し、それを運用するセンタ集中管理が存在する。このようなサービスでの個人データの運用には、例えば、個人ユーザから興味ある分野の情報を収集していると、その分野の企業と契約し、代理広告をするといったものがある。従来のこのような集中管理の形態では、センタが個人情報を管理して、個人データは、センタから第三者に提供をするといったことはなかった。

【００１３】

また、個人情報ではないが、著作権保護に関し、最近では、ＤＲＭ（Digital Rights Management）という技術が使用されている。ＤＲＭとは、利用許可条件とその条件に従って動作する機構からなっている。利用許可条件には、例えば、利用回数や利用期限、コピー回数などがある。（下記、非特許文献１、２参照）

従来の電子データのプライバシーに関すると取り組みとしては、ユーザが、Cookieなどのデジタル・オブジェクトや実行ファイルについて受け入れるか拒否することを指定可能とする技術がある（特許文献１参照）。また、個人情報管理センタが個人情報提供者と個人情報利用者との仲立ちを行う構成を有する技術がある（特許文献２参照）。

【００１４】

【特許文献１】

特表平１０－５１２０７４号公報（米国特許６，３６３，４８８号明細書）

【００１５】

【特許文献２】

特開２００１－２６５７７１号公報

【００１６】

【非特許文献１】

穴澤健明、武村浩司、常広隆司、長谷部高行、畠山卓久：コンテンツ保護の柔軟化を実現した開放型超流通基盤、情報処理学会　電子化知的財産・社会基盤研究会報告、２００１年１１月＜online＞http://www.keitaide-music.org/pdf/EIP14-5.pdf

【００１７】

【非特許文献２】

畠山卓久、丸山秀史、千葉哲央：音楽コンテンツの超流通とセキュリティ．ＦＵＪＩＴＳＵ，Vol.52,No.5, p.473-481, 2001年9月．http://magazine.fujitsu.com/

【００１８】

【発明が解決しようとする課題】

１）個人情報保護に関して上記従来技術で挙げた（２）及び（３）の（ウ）の対策では、正当なアクセス権を持っているものが、勝手に情報をコピーしたり、改ざんしたり、削除したりするといった不正な使用が可能である。

２）上記従来技術で挙げた（１）に対して、目的範囲内での使用は、正当なアクセス権を持っているものに対して個人情報規定などといった行動規範による対策しか行われておらず、実質的に目的外使用に関しては、情報処理技術による対策は存在しない。

３）従来技術で挙げた要件（５）に対する解決策は、センタだけが個人データを保有し、管理するといった形態の解決方法である。したがって、センタが個人データを第三者に提供した後、個人データが点在するような環境において開示・訂正・削除といった対策は存在しない。

４）上記センタ集中管理による個人情報取り扱いに関するサービスでは、センタ

から一旦個人データを事業者に提供してしまうと、提供された事業者は、他の事業者へ不正に販売するなど、現在のところセンタから第三者へ個人データを提供するということはしない。

【００１９】

本発明の課題は、情報主体の制御の下、個人情報の流通を情報主体の意思に従って制御することができる個人情報保護流通システムを提供することである。

【００２０】

【課題を解決するための手段】

本発明の個人データ保護流通方法は、暗号化された個人データを受信するステップと、暗号化された、該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを受信するステップと、前記復号鍵と個人データ使用ライセンスを復号するステップと、前記個人データの用途が前記個人データ使用ライセンスに記述された使用条件と一致するかを判断するステップと、前記個人データの用途が前記使用条件と一致するときのみに前記復号された復号鍵を用いて前記個人データを復号するステップとを有することを特徴とする。

【００２１】

したがって、本発明によれば、個人データの取得者の個人データの使用方法を、個人データの提供者（情報主体）が、自ら個人データ使用ライセンスを作成することによって、制限することができる。したがって、個人データの提供者の制御の下に、提供者の個人データが流通することになるので、個人データの提供者は、自分の個人データが思わぬところで不正に使用されることを防止することができる。

【００２２】

【発明の実施の形態】

本発明の実施形態においては、以下のような構成を採用する。

1）不正な使用の禁止に関しては、ＴＲＭ（Tamper　Resistant　Module）化したＤＲＭ（Digital　Rights　Management）でしか利用できないようにすることにより、改ざんや削除が禁止される。このとき、更に使用ライセンスの使用条件

にＴＲＭ化したＤＲＭ装置を移動する毎に移動回数が１ずつ減るような移動可能回数を設け、かつ、使用ライセンスに、コピー可能条件を設けないかあるいは、設けても０と設定することにより、不正コピーが禁止される。

２）目的外使用に関しては、使用ライセンスの使用目的という条件により解決される。具体的には、個人データを利用するアプリケーションを使用目的別に分類し、各アプリケーションの使用目的が識別できる状態にしておき、個人データを使用するときに、その使用ライセンスの使用条件に対応するアプリケーションでしか利用できないようなＤＲＭ機構を備えておく。

３）情報主体からの個人データの情報主体への開示請求においては、センタ（事業者の一種であるが、個人データの管理を主な業務としている事業者である）への開示請求によって実現できる。そして、センタが個人データを提供した他の事業者に関しては、センタが作成した個人データをどの事業者に提供したかのリストを情報主体に提供することにより、その情報主体の個人データを保有している全ての事業者に対して、情報主体が開示請求を行うことを可能にする。

【００２３】

個人データの訂正請求に関しては、情報主体は、センタに個人データの訂正要求を出し、訂正の後の個人データの訂正情報が各事業者間で同期され解決される（ここで、同期とは、各事業者間で同じ個人データを有するように、各事業者に対し個人データの更新を行うことを示す）。

【００２４】

個人データの削除請求に関しては、情報主体は、個人データを記載した名簿リストから削除してもらいたい事業者を特定し、その事業者の名簿リストから自分の個人データを直接削除してもらうことにより解決される。あるいは、センタに個人データの削除要求を出し、センタにある名簿リストから削除してもらう。このとき、センタの名簿リストが削除されたことにより、センタから名簿リストの提供を受けた事業者の保有する名簿リストに対しても、同様の削除が行われる。

４）上記３つの手段をセンタ及びセンタが個人データを提供する事業者に適用し、情報主体には、クライアントコンピュータを設置することにより安全な個人データの流通が可能になる。このとき、ライセンスの価格を設定するなどしてビジ

ネスとして商業ベースにのせることもできる。なお、センタが事業者に個人データを提供するときは、名簿リスト単位で事業者に提供する。

１．概要

１．１問題提起

図１は、情報主体、事業者、第三者の関係を説明する図である。

【００２５】

情報主体、事業者、第三者の３者からなる構成を考える。情報主体、事業者、第三者は、それぞれ、ネットワークで接続されたコンピュータを有している。事業者は、そのコンピュータの個人情報データベースに情報主体の個人データを持っている。第三者は、情報主体の個人データを取得したい要求がある。

【００２６】

そこでまず、情報主体と事業者との間において以下のことが満足していなくてはならない。

[事業者の情報主体に対する要件]

（１）事業者は、情報主体に対して個人データの使用目的を告知し、その目的範囲内で使用しなければならない。（目的外使用・不正使用の禁止）

（２）事業者は、不正に個人データを提供してはならない。（不正提供・二次使用の禁止）

（３）事業者は、個人データを安全に保管しなくてはならない。（安全な保管）

（４）事業者は、個人データを安全に収集しなければならない。（安全な収集）

（５）事業者は、情報主体に対して、要求があった場合には、いつでもその情報主体の個人データを開示したり、訂正したり、削除しなければならない。（情報主体のコントロール権の確保）

これら４つの要件を満足した上で、事業者は、第三者に個人データを提供する。このときも、第三者は、事業者に対して、少なくとも上記要件と同様なことが満足されなければならない。すなわち、

[第三者の事業者に対する要件]

（６）第三者は、情報主体に対して個人データの使用目的を告知し、その目的範囲内で使用しなければならない。（目的外使用・不正使用の禁止）

（７）第三者は、不正に個人データを提供してはならない。（不正提供・二次使用の禁止）

（８）第三者は、個人データを安全に保管しなければならない。（安全な保管）

（９）第三者は、個人データを安全に収集しなくてはならない。（安全な収集）

（１０）第三者は、情報主体に対して、要求があった場合にはいつでもその情報主体の個人データを開示したり、訂正したり、削除しなければならない。（情報主体のコントロール権の確保）

である。

【００２７】

本発明の実施形態では、これら１０個の要件を満足する実現法を提案する。

１．２解決方法の概要

１．１節の問題に対する解決法として以下のようにする。

【００２８】

図２は、本発明の実施形態の構成の概略構成を説明する図である。

基本的には、個人データの使用にＤＲＭ技術を利用する。すなわち、個人データを暗号化し、その暗号化個人データの使用ライセンスを発行し（ライセンスを発行できるのは、情報主体のみ）、個人データを利用するときには、ＤＲＭ機能をもつアプリケーションでしか利用できないようにする。このようにすることで、まず、個人データの不正使用（二次使用・目的外使用）が制御できる。

【００２９】

また、事業者たちが使用ライセンスを保管し、利用する装置をＴＲＭ化することにより、個人データの安全な保管が実現され、更にライセンスを送受するときに暗号通信をすることにより個人データの安全な収集が可能である。

【００３０】

そして、事業者たちは開示、訂正、削除といったサービスを情報主体に提供することで、情報主体のコントロール権を確保する。

すなわち、

情報主体

・個人データを暗号化する

・個人データの使用条件である使用ライセンスを発行する。

・ライセンスを暗号通信で送信する。

事業者、第三者

・ライセンスを送受するときは暗号通信を用いる。

・ライセンスは、ＴＲＭ化されたＤＲＭ認証機能を有するユニットに保管する。

・ＤＲＭ認証機能を持つ適切なアプリケーションで個人データを使用する。

・情報主体による個人データの開示・訂正・削除請求に応じる。

２．情報主体－事業者間での個人データの保護

サービス事業者（個人データの管理を主に行う事業者ではなく、個人データの利用を目的とする事業者）が情報主体へ個人情報の提供を要求する場合、一般的には以下のようなやりとりが行われる。

（１）個人情報提供要求

・サービス業者から情報主体へ個人情報を提供するよう要求する。

・このとき、サービス業者は、情報主体へ「サービス業者の名称」、「問い合わせ先」、「提供してもらう個人情報の項目」、「利用目的」などの情報を通知する。

・また、提供した場合どのようなサービスが受けられるかなどの情報も通知する。

（２）個人情報の提供の意思決定

・情報主体は、サービス業者から受け取った情報から、個人情報を提供するかどうかを判断する。

（３）個人情報提供

・提供する場合、情報主体は、自分の個人データを作成し、サービス業者へ提供する。

（４）個人情報を利用する

・サービス業者は、受け取った個人情報を情報主体に提示した利用目的の範囲内で利用する。

【００３１】

以上が一般的な個人情報提供の手続きであるが、本発明の実施形態では（３）

と（４）を以下に示すような仕組みを用いることにより、遠隔から個人情報の不正な使用・目的外使用の制御を実現する。

２．１．個人情報の提供と個人情報利用の仕組み

図３は、情報主体が個人情報を提供することに同意した場合の提供の仕組みと、サービス業者がその情報を利用する仕組みを示す図である。

【００３２】

個人データ１０は、情報主体の持つコンピュータのクライアントツール２０が生成した共通鍵暗号方式の鍵１１を使って暗号化され、その暗号化個人データは、サービス業者のコンピュータ２１の個人データ・データベースシステム２２にネットワーク２５を介して送られ、アプリケーション２４が個人データを利用するときに、アプリケーション１０にロードされ、復号される。

【００３３】

個人データ使用ライセンス１２には、個人データ１０を暗号化するのに使用した共通鍵暗号方式の暗号鍵１１が入り、サービス業者のコンピュータ２１に設けられるライセンスデータベースシステム２３に、ネットワーク２５を介して送信される。このとき、個人データ使用ライセンス１２は、ライセンスデータベースシステム２３の公開鍵暗号方式の公開鍵１４と、ＤＲＭ認証に使用されるセッション鍵１３とで、二重に暗号化されて、ライセンスデータベースシステム２３に送信される。

２．１．１．情報主体による個人情報の編集

更に、図３を参照して説明を続ける。

【００３４】

情報主体２０は、個人データ１０を編集し、その個人データ１０に対して公開鍵暗号方式で暗号化する。暗号化は、住所、電話番号といった個人情報の各項目に対して鍵を生成し暗号化する。そして、個人データ使用ライセンス１２を作成する。このとき、個人データ使用ライセンス１２に、個人情報を暗号化したときの鍵１１が含まれる。これらの処理は、情報主体のクライアントツール２０により実行される。クライアントツールの機能としては、以下のものがある。

・使用ライセンスを発行する機能

・共通鍵暗号方式により個人データ１０を暗号化・復号化する機能

・暗号鍵１３を生成する機能

・暗号化個人データを受け渡す機能

・個人データ使用ライセンス１２を送信する機能（ＤＲＭ認証ができる機能）

［個人データ使用ライセンス］

個人データ使用ライセンス１２とは、個人データ１０の使用条件を表現したものであり、個人データ１０を利用する側は、この条件にしたがって実行される機構を持つアプリケーション２４で使用する。

【００３５】

個人データ使用ライセンス１２には、暗号化個人データ１０を復号するための復号鍵１１と、その復号鍵で復号される暗号化個人データ１０の識別子、そして使用条件から構成される。使用条件は、具体的には、以下のようなものがある。ただし、使用条件にはコピー回数は含めず、ライセンスをコピーすることはできないようにする。

・使用回数

情報主体２０は、自分の個人データ１０を利用する回数を制限できる。

・使用期限

情報主体２０は、使用期限を指定できる。使用期限が過ぎたら、個人データ１０の利用者側のライセンスデータベースシステム２３から個人データ使用ライセンス１２が強制的に削除される。

【００３６】

情報主体２０が個人データ１０提供した相手に対して個人データ１０の使用有効期限を決定することができる。

・移動回数

個人データ使用ライセンス１２の、ＤＲＭ認証機能のついた装置間の移動回数を制限する。ＤＲＭ認証をする度毎に、サービス業者のコンピュータ２１に移動回数を計数するために設けられたカウンタの値が１ずつ減る。

・使用目的

少なくとも、以下の使用目的属性を設ける。

－調査と開発

　個人データ１０は、製品調査や、開発など、統計をとるようなアプリケーション２４で実行される。

－貸与・販売

－データマイニング

　データマイニングするツールで実行される。

・提供許可業者

ライセンスを提供してもよい業種を記する。

・提供拒否サービス

　どのようなサービスを受けたくないかを記述する。

・印刷回数

　個人データ１０を印刷して良い回数を記述する。

【００３７】

図４は、使用条件と個人データの使用との関係を説明する図である。

上記した使用条件は、図４のように、個人データ使用ライセンスを提供するとき、及び個人データを使用するときに、参照され、個人データを使用する状況と使用条件のマッチングを行うことにより、ライセンスの提供・個人データの使用を制限する。

【００３８】

すなわち、クライアントツールあるいは、第１のサービス業者から、第２のサービス業者に個人データが送信される場合には、個人データ使用ライセンスの使用条件である（１）提供許可業者にあたるか、（２）提供拒否サービスにあたるか、について判断し、提供可能な場合のみ個人データ使用ライセンスを提供する。また、第２のサービス業者のコンピュータのライセンスデータベースシステムから、第２のサービス業者のコンピュータ内のアプリケーションに個人データを移動する場合には、個人データ使用ライセンスの使用条件の移動回数を参照し、指定された回数以内で、個人データを移動できるか否かを判断し、個人データを移動するか否かを判断する。また、アプリケーションでは、個人データを使用する場合、個人データ使用ライセンスの（１）使用目的、（２）使用回数、（３）

使用期限などの条件を満たして、個人データを使用できるか否かを判断し、個人データを使用するか否かを決定する。

２．１．２情報主体からの個人情報の提供

図３において、情報主体２０は、暗号化された個人データ１０と個人データ使用ライセンス１２を作成した後、暗号化個人データをサービス業者２１が保持している個人データ・データベースシステム２２へ送り、個人データ使用ライセンス１２をライセンスデータベースシステム２３へ送る。個人データ・データベースシステム２２及びライセンスデータベースシステム２３へは、サービス業者２１の従業員でも、特定のアクセス権を持つ者しかアクセスできない。個人データ使用ライセンス１２を保存する装置は、すべてＴＲＭ化されているとする。

【００３９】

個人データ使用ライセンス１２の提供に関しては、ＤＲＭ認証を用いる。

実際の利用場面において、サービス業者２１は、利用期限・回数がなくなったときに、情報主体２０に個人データ使用ライセンス１２の継続使用についての要求を出し、情報主体２０は、それに対して、受理・拒否の応答することを想定している。したがって、情報主体２０がサービス業者２１に個人データ１０を提供する際、情報主体２０は、利便性を考慮して、適当な使用期限や使用回数を設定した個人データ使用ライセンス１２をサービス業者２１に提供する。

２．１．３．サービス業者による個人情報の利用

サービス業者２１は、個人データ提供要求のときに示した利用目的に合致したとき、ＴＲＭ化された装置のＤＲＭ機能を持ったアプリケーション２４でのみ個人データ１０を利用できる。すなわち、図３において、暗号化された個人データ１０は、個人データ・データベースシステム２２からアプリケーション２４に渡されるが、同時にライセンスデータベースシステム２３に格納されている個人データ使用ライセンス１２が秘密鍵１５によって暗号化され、アプリケーション２４に渡される。アプリケーション２４では、暗号化された個人データ使用ライセンス１２をＤＲＭ認証し、アプリケーション２４において、個人データ使用ライセンス１２を解読し、個人データ１０の復号鍵１１を取り出して、個人データ１０をこの復号鍵１１で復号して使用する。なお、このアプリケーション２４は、

目的ラベルを持っており、その値が個人データ使用ライセンス１２の目的属性と合致しない場合、その個人データ１０を使用できないようになっている。ここで、アプリケーション２４が持つ目的ラベルとは、個人データ使用ライセンス１２の使用目的属性を値域に持つ変数であり、アプリケーション作成メーカが、予めそのアプリケーション２４に設定する、あるいは、プラグインなどで、この値が設定されることを想定する。

【００４０】

図５は、ＤＲＭ認証を説明する図である。

ＤＲＭ認証は、図５に示すように、セッション鍵２（秘密鍵）を共有するためのプロトコルである。

【００４１】

以下のＤＲＭ認証の説明においては、サービス業者のコンピュータと情報主体のクライアントツールとの間でＤＲＭ認証が行われるものとして説明する。まず、サービス業者のコンピュータから個人データの取得要求とサービス業者の証明書がクライアントツールに送られる（①）。次に、クライアントツールは、送られてきたサービス業者の証明書の検証を行い（②）、セッション鍵１を生成する（③）。そして、クライアントツールは、セッション鍵１をサービス業者のコンピュータに送り（④）、サービス業者のコンピュータは、セッション鍵２を生成する（⑤）。そして、セッション鍵１で暗号化して、セッション鍵２をクライアントツールに送信する（⑥）。

【００４２】

ここで、④では、セッション鍵１をサービス業者の証明書にある公開鍵で暗号化し、送信する。⑥では、セッション鍵２は、セッション鍵１により共通鍵暗号方式により暗号化して送信される。

【００４３】

図６は、クライアントツールの個人データ使用ライセンスの送信時のフローチャートである。

まず、ステップＳ１０において、個人データ要求の受信が行われる。ステップＳ１１では、個人データを提供するか否かを決定する。個人データを提供しない

場合には、ステップＳ１２において、エラー処理を行い、処理を終了する。ステップＳ１１において、個人データを提供すると決定された場合には、ステップ１３に進み、個人データを作成する。そして、ステップＳ１４において、共通鍵暗号方式の鍵を生成し、ステップＳ１５において、個人データを暗号化する。そして、ステップＳ１６において、個人データ使用ライセンスを生成し、ステップＳ１７において、暗号化個人データを送信する。ステップＳ１７においては、暗号化された個人データをＤＲＭ認証し、ＤＲＭ認証が無効の場合には、ステップＳ１９において、エラー処理を行い、処理を終了する。ステップＳ１８のＤＲＭ認証において、認証結果が有効と判断された場合には、ステップＳ２０において、個人データ使用ライセンスを送信して、処理を終了する。

【００４４】

図７は、個人データと個人データ使用ライセンスとの関係を説明する図である。

個人データを使用する際には、暗号化個人データの他に、個人データ使用ライセンスが用いられ、個人データ使用ライセンスの使用目的に「データマイニング」が設定されていた場合、個人データを使用するサービス業者側のアプリケーションでは、その目的ラベルに「データマイニング」が設定されていないと、使用できない仕組みとなっている。

【００４５】

図８は、サービス業者のコンピュータのアプリケーションで個人データを使用する際のフローチャートである。

まず、ステップＳ３０において、アプリケーションは、暗号化個人データをロードする。ステップＳ３１では、ライセンスデータベースシステムから対応する個人データ使用ライセンスを受信し、個人データ使用ライセンスが有効か否かを判断する。ステップＳ３１において、無効と判断された場合には、ステップＳ３２において、アプリケーションは、個人データの使用拒否通知を受信し、処理を終了する。このとき、ライセンスの移動回数は増やされない。

【００４６】

ステップＳ３１において、有効と判断された場合には、ステップＳ３３におい

て、個人データ使用ライセンスの移動可能通知を受信する。すなわち、今回の移動が許容される移動回数内の移動であることを確認する。そして、ステップＳ３４において、個人データ使用ライセンスのＤＲＭ認証を行う。この認証が無効となった場合には、ステップＳ３５において、エラー処理をする。ステップＳ３４において、ＤＲＭ認証の結果が有効となった場合には、個人データ使用ライセンスをステップＳ３６において、受信し、ステップＳ３７において、アプリケーションの使用目的と個人データ使用ライセンスの使用目的が一致するか否かを判断する。ステップＳ３７において、一致しないと判断された場合には、ステップＳ３８において、個人データ使用ライセンスをライセンスデータベースシステムに戻して、処理を終了する。

【００４７】

ステップＳ３７において、一致すると判断された場合には、ステップＳ３９において、個人データ使用ライセンスの使用回数と使用期限が有効か否かを判断する。ステップＳ３９において、無効と判断された場合には、ステップＳ４０において、個人データ使用ライセンスをライセンスデータベースシステムに戻して、処理を終了する。ステップＳ３９において、有効と判断された場合には、ステップＳ４１において、個人データの復号を行い、個人データ使用ライセンスの使用可能回数を１回分差し引く。そして、ステップＳ４２において、個人データを使用し、ステップＳ４３において、個人データの使用が完了すると処理を終了する。

【００４８】

図９は、ライセンスデータベースシステムのライセンス送信時のフローチャートである。

まず、ステップＳ５０において、アプリケーションから個人データ使用ライセンスの取得要求を受信する。ステップＳ５１において、要求された個人データ使用ライセンスは、移動可能か否かを判断する。ステップＳ５１において、移動が不可能と判断された場合には、ステップＳ５２において、アプリケーションへ個人データ使用ライセンスの移動拒否通知を行い、処理を終了する。ステップＳ５１において、移動が可能とされた場合には、ステップＳ５３において、移動可能

通知をアプリケーションに送信する。そして、ステップＳ５４において、個人データ使用ライセンスのＤＲＭ認証を行う。ステップＳ５４の認証の結果、無効となった場合には、エラー処理をステップＳ５５において行い、処理を終了する。ステップＳ５４において、ＤＲＭ認証の結果、有効と判断された場合には、ステップＳ５６において、個人データ使用ライセンスをアプリケーションに送信（移動）して、処理を終了する。

【００４９】

図１０は、本発明の実施形態の別の構成における適用例を説明する図である。

図１０においては、情報主体２０からサービス業者１（センタのコンピュータ）が個人データと個人データ使用ライセンスを受け取り、保管して、他のサービス業者２のコンピュータ２１ａから個人データの使用要求を受け付け、個人データをサービス業者２に提供する構成を示している。なお、図３と同じ構成要素には同じ参照番号を付している。

【００５０】

サービス業者２のコンピュータ２１がサービス業者２のコンピュータ２１ａから個人データの取得要求を受け取ると、暗号化された個人データをサービス業者２のコンピュータ２１ａの個人データ・データベースシステム２２ａに送ると共に、個人データ使用ライセンスをＤＲＭ認証のためのセッション鍵と公開鍵方式の暗号鍵で暗号化して、ライセンスデータベースシステム２３ａに送信する。暗号化された個人データと個人データ使用ライセンスを受け取ったサービス業者２のコンピュータ２１ａにおける個人データの使用は、図３において説明したものと同様であるので、説明を省略する。

【００５１】

このように、本発明の実施形態においては、サービス業者１のように、個人データの管理を主に行い、他のサービス業者からの個人データの取得要求に応じて、個人データ使用ライセンスとともに、個人データを提供する構成が可能である。この場合、サービス業者１は、個人データ管理センタとなるものである。

２．２．開示請求

個人データ１０を扱っているサービス業者２１は、個人データ１０を提供して

いる情報主体２０から開示請求（個人データ１０を情報主体２０に提示すること）があった場合、情報主体２０に対して個人データ１０を開示しなければならない。図１１は、情報主体から開示請求があった場合の開示の仕組みを示す図である。

①個人データ開示要求

・情報主体は、サービス業者へ自分の個人データの開示を要求する。

②暗号化個人データ＋サービス業者作成データの送信

・サービス業者は個人データ・データベースシステムから暗号化された状態の個人データとその情報主体に関する関連したサービス業者が作成したデータを情報主体にむけて送信する。例えば、サービス業者作成データには、サービス業者が銀行である場合、口座の残高情報などがある。

・なお、サービス業者作成データは、その情報の内容により、暗号化される場合もある。

③復号

・情報主体は、以前に自分の個人データを暗号化した鍵で復号し、情報を見る。

２．３．訂正請求

個人データを扱っているサービス業者は、個人データを提供している情報主体から当該個人データの訂正請求があった場合、本人の要求かどうかを確認し、情報主体が要求するないように訂正しなければならない。

【００５２】

図１２は、情報主体からの個人データの訂正請求における動作を説明する図である。

①個人データ訂正要求

・情報主体は、サービス業者へ自分の個人データの訂正を要求する。

②暗号化

・情報主体は、自分の個人データを訂正したものを用意し、新たに暗号化鍵を生成し、訂正した個人データを暗号化する。

③暗号化個人データの送信

・情報主体は、暗号化した個人データをサービス業者に向けて送信する。

・サービス業者は、訂正前の暗号化個人データを削除し、新しいデータに更新する。

④個人情報使用ライセンスの提供

・情報主体は、暗号化鍵の情報が更新された個人データ使用ライセンスをサービス業者に提供する。

・サービス業者は、訂正前のライセンスを削除し、新しいものに更新する。

【００５３】

図１３は、サービス業者側の個人データの訂正処理のフローチャートである。

まず、ステップＳ６０において、訂正要求を情報主体から受信する。ステップＳ６１において、ユーザ認証を行い、訂正要求をしてきた情報主体であるユーザは、登録者か否かを判断する。ステップＳ６１において、ユーザが登録者でないと判断された場合には、ステップＳ６２において、エラー処理を行い、ステップＳ６３において、訂正要求をしてきた者へ要求拒否通知を送信して、処理を終了する。

【００５４】

ステップＳ６１において、ユーザが登録者であると確認された場合には、ステップＳ６４において、情報主体であるユーザに訂正データを要求する。そして、ステップＳ６５において、訂正された暗号化個人データを受信し、ステップＳ６６において、暗号化個人データの更新を行う。ステップＳ６７において、個人データ使用ライセンスのＤＲＭ認証を行い、認証の結果が無効の場合には、エラー処理（ステップＳ６８）、要求者への要求拒否通知の送信（ステップＳ６９）を行って、処理を終了する。ステップＳ６７において、ＤＲＭ認証の結果が有効である場合には、ステップＳ７０では、個人データ使用ライセンスを受信し、個人データ使用ライセンスを更新し（ステップＳ７１）、ステップＳ７２において、要求者へ訂正完了通知を送信して、処理を終了する。

２．４．削除請求

基本的には、２．３節の訂正要求と同じことをする。異なる点は、訂正要求では、訂正した暗号化個人データと訂正した個人データ使用ライセンスを使って、以前に使用していたものを削除してから更新したが、削除請求の場合は、この更

新処理がいらないというところである。すなわち、単に、サービス事業者の有する暗号化個人データと個人データ使用ライセンスを削除するだけである。

【００５５】

情報主体が削除命令を強制する方法として以下が挙げられる。

[情報主体と個人データを取り扱うサービス業者との契約による削除]

情報主体は、例えば、ライセンスの使用条件を期間で限定する、あるいは、使用回数で制限する。こうすることにより、それを使っている個人データ取り扱いサービス業者は、使用回数や使用期間などの更新のために、情報主体に問い合わせに来る。そのときに、情報主体は、使用の継続を許可するかどうかを決定する。もし情報主体が、継続の許可をしなければ、個人データ取り扱いサービス業者は、その情報主体の個人データを使用することができなくなり、事実上、削除したことと同じになる。

[ライセンス代理提供サーバによる削除]

図１４は、ライセンス代理提供サーバによる個人データの削除処理を説明する図である。

【００５６】

情報主体は、信頼できるライセンス代理提供サーバに暗号化個人データ、個人データ使用ライセンスを発行し、このサーバがサービス業者の要求に対して、情報主体の同意を得た上で、個人データ使用ライセンスを提供する。このサーバは、常時接続の状態にある。したがって、サービス業者は、いつでもサーバにアクセスして、個人データを要求することができる。個人データ使用ライセンスは、短い期間、例えば、１日単位などでその使用条件を制限すれば、サービス業者は、個人データ使用ライセンスを更新するため、毎日ライセンス代理提供サーバにライセンスを要求してくることになる。したがって、情報主体がサービス業者に削除を請求する場合、情報主体は、ライセンス代理提供サーバに削除請求し、ライセンス代理提供サーバは、以後サービス業者にライセンスを発行しないことにより、情報主体の削除請求を実現する。

【００５７】

すなわち、以下のような処理の流れとなる。

①情報主体がクライアントツールを使って、ライセンス代理提供サーバに削除請求をする。

②サービス業者は、個人データを使用するために、個人データ使用ライセンスをライセンス代理提供サーバに要求する。

③しかし、ライセンス代理提供サーバは、情報主体から削除請求を受け取っているので、サービス業者に対して、個人データ使用ライセンスを発行しない。これにより、サービス業者は、当該情報主体の個人データを使用できなくなる。

２．５．個人情報を名簿単位で使用する

サービス業者は、大量の個人データを保持しているので、実際には、一人一人個別に個人データを使用するというよりも、ある単位でまとめた個人データを名簿として扱い、これを利用する。ここでは、このような名簿を使用するための仕組みについて説明する。

２．５．１．名簿の作成と名簿ライセンスの生成

名簿は、個人データ使用ライセンスに含まれる使用条件の内、同一の使用条件となっている暗号化個人データを連結して、個人データ名簿として名簿データベースの中で保存される。これは、ライセンスデータベースに入っている個人データ使用ライセンスが更新される度に、個人データ使用ライセンスの内、同一の使用条件を有するものを集めて、整頓する。一つの同一使用条件の個人データ使用ライセンスのリストを名簿ライセンスと呼ぶ。この名簿ライセンスにある個人データを識別するＩＤに基づいて、暗号化個人データが表１のように、個人データ名簿となる。

【００５８】

【表１】

| ID | 氏名 | 性別 | 生年月日 | メールアドレス | 電話番号 | 職業 | ・・・ | 興味ある分野 |
|---|---|---|---|---|---|---|---|---|
| 0001 | ○○○ | 男 | ○年○月○日 | ○○@○○○ | ○○○−○○○ | エンジニア | ・・・ | スポーツ |
| 0002 | △△△ | 男 | △年△月△日 | △△@△△△ | △△△−△△△ | 教員 | ・・・ | サイエンス |
| ・<br>・<br>・ | ・<br>・<br>・ | ・<br>・<br>・ | ・<br>・<br>・ | ・<br>・<br>・ | ・<br>・<br>・ | ・<br>・<br>・ | ・<br>・<br>・ | ・<br>・<br>・ |
| 1111 | ×××× | 女 | ×年×月×日 | ××@×××× | ×××−×××× | 学生 | ・・・ | 旅行 |

【００５９】

なお、ここで、個人データ名簿のＩＤ以外の項目は暗号化される。

また、名簿ライセンスについては、図１５のように生成する。

図１５は、名簿ライセンスの生成処理を説明する図である。

【００６０】

各同一使用条件の個人データ使用ライセンスを組にし、それらに含まれる暗号化鍵を連結する。連結した鍵を使用条件と一緒にし、名簿ライセンスを生成する。このとき、名簿ライセンスそのものを識別し、かつ名簿ライセンスから名簿が参照できるよう識別子であるライセンス－名簿ＩＤが付与される。

【００６１】

生成された名簿ライセンスは、名簿ライセンスデータベースシステムに保存される。したがって、名簿ライセンスデータベースは、表２のようなエンティティのリストが保存されている。

【００６２】

【表２】

| | | | |
|---|---|---|---|
| ライセンス－名簿ID | | XXX | |
| 条件 | 使用回数 | 100 | |
| | 使用期限 | 2003年3月31日 | |
| | 移動回数 | 100 | |
| | 使用目的 | マイニング | |
| | 提供可能業者 | メーカー | |
| | 提供拒否サービス | ダイレクトメール | |
| ライセンスID＋鍵 | | X1 | 101000101 |
| | | X2 | 1100001111 |
| | | ・<br>・<br>・ | ・<br>・<br>・ |
| | | X1000 | 010101011 |
| 名簿ライセンスの鍵（連結された鍵） | | 101000101\|\|1100001111\|\|・・・\|\|010101011 | |

【００６３】

これらの処理は、名簿作成ツールが行う。ライセンスデータベースと名簿ライセンスデータベースは、物理的には同じデータベースシステム上にあってもよい

。

【００６４】

図１６は、名簿の作成と名簿ライセンスの生成処理を図示した模式図である。

サービス業者は、複数の情報主体のコンピュータから、暗号化された個人データを収集し、個人データ・データベースに格納する。また、サービス業者は、各情報主体のコンピュータから個人データ使用ライセンスを受信し、ライセンスデータベースに格納する。名簿作成ツールは、ライセンスデータベースを参照し、同じ使用条件を持っている個人データを個人データ・データベースから探しだし、名簿にして名簿データベースに格納する。また、各個人データ使用ライセンスは、名簿作成ツールが、上記のようにして、名簿ライセンスにして、名簿ライセンスデータベースに格納する。なお、ここで、名簿作成ツール、ライセンスデータベース、及び名簿ライセンスデータベースはＴＲＭ化されたＤＲＭ機能を有する装置である。

【００６５】

図１７は、名簿作成ツールが名簿・名簿ライセンスを作成する処理のフローチャートである。

まず、ステップＳ８０において、全ての個人データ使用ライセンスをロードする。次に、ステップＳ８１において、個人データ使用ライセンスを使用条件別にソートする。ステップＳ８２においては、同一使用条件の個人データ使用ライセンスを連結し、名簿ライセンスを作成する。ステップＳ８３では、名簿ライセンスの個人データＩＤを取得し、ステップＳ８４において、個人データＩＤから暗号化名簿の作成を、個人データ・データベースに要求する。そして、ステップＳ８５において、名簿ライセンスを名簿ライセンスデータベースに保存して、処理を終了する。

２．５．２．名簿の使用

名簿の使用も基本的には、２．１．３節と同じくＴＲＭ化された装置のＤＲＭ認証機能を持ったアプリケーション内でしか使用できない。

【００６６】

図１８は、名簿の使用形態を説明する図である。

サービス業者は、名簿データベースからアプリケーションに名簿をロードするが、同時に、ＤＲＭ認証機能を使って、名簿ライセンスデータベースに補間されている名簿ライセンスをアプリケーションに渡す。そして、アプリケーションは、名簿ライセンスに従って、名簿を復号化して使用する。

２．６．名簿を使用する場合の開示請求

サービス業者が、名簿を使用する場合、情報主体からの開示請求に対してサービス業者は、個人情報データベースシステムに保存されている暗号化個人データとその情報主体の付加情報を合わせて送信する。従って、開示に関しては、２．２節と同様な方法となる。

２．７名簿を使用する場合の訂正請求

名簿を使用する場合の個人情報を訂正するには、サービス業者は、個人データ・データベースシステムの古い個人データを削除し、訂正して個人データを受け取る。その後、名簿データベースシステムの関係する名簿の情報主体の項目を削除し、訂正した内容に変更する。個人データ使用ライセンスについても同様に、ライセンスデータベースシステムの古い個人データ使用ライセンスを削除し、訂正した個人データ使用ライセンスに変更する。その後、名簿ライセンスデータベースシステムの関係する名簿ライセンスの鍵を変更する。ただし、ライセンスに関しての変更点は、個人データを変更した項目における鍵であり、使用条件については変更しない。したがって、名簿ライセンスの変更個所は、鍵のみとなる。

【００６７】

図１９は、名簿使用時の訂正要求の処理を説明する図である。

①クライアントツールからサービス業者に個人データの訂正要求が送信される。

②訂正した暗号化個人データを送信する。

③サービス業者の個人情報データベースにおいて、個人データを訂正する。

④次に、名簿データベースの名簿を訂正する。

⑤クライアントツールから訂正した個人データ使用ライセンスをサービス業者に送信する。

⑥ライセンスデータベースにおいて、個人データ使用ライセンスを訂正する。

⑦名簿ライセンスデータベースの名簿ライセンスを訂正する。

⑧サービス業者からクライアントツールに訂正完了通知が通知される。

【００６８】

図２０は、名簿使用時のサービス業者の名簿の訂正処理を示すフローチャートである。

まず、ステップＳ８９において、訂正要求を受信する。ステップＳ９０において、訂正要求をしてきた、情報主体である要求者は登録者であるか否かを判断する。ステップＳ９０の判断がＮＯの場合には、エラー処理をステップＳ９１において行い、ステップＳ９２において、要求者へ要求拒否通知を送信する。

【００６９】

ステップＳ９０の判断がＹＥＳの場合には、ステップＳ９３において、訂正データを要求者に要求する。ステップＳ９４において、訂正された暗号化データを受信し、ステップＳ９５において、個人データ・データベースを更新し、ステップＳ９６において、名簿データベースを更新する。

【００７０】

ステップＳ９７においては、個人データ使用ライセンスの送受信のためのＤＲＭ認証を行う。ステップＳ９７の結果が無効である場合には、ステップＳ９８において、エラー処理を行い、ステップＳ９９において、要求者へ要求拒否通知を送信する。ステップＳ９７の結果が有効である場合には、ステップＳ１００において、個人データ使用ライセンスを要求者から受け取り、ステップＳ１０１において、ライセンスデータベースを更新する。そして、ステップＳ１０２において、名簿ライセンスデータベースを更新し、ステップＳ１０３において、要求者へ訂正完了通知を送信して処理を終了する。

２．８名簿を使用する場合の削除請求

名簿を使用する場合における情報主体の個人データを削除する手順は、２．７節の訂正請求とほぼ同様である。異なるところは、訂正の場合は、訂正した個人データに変更するが、削除の場合は、その処理はいらない。

３．サービス業者間での個人データの保護

図２１は、サービス業者間で個人データを取り引きする処理を示す図である。

【００７１】

サービス業者間で個人データを取り引きする場合、必ず情報主体に提供してよい旨の同意を得る必要がある。サービス業者Ａが、ある情報主体の個人データを保有していると仮定し、サービス業者Ｂにその個人データを提供する場合を考える。

３．１サービス業者間におけるライセンス提供の仕組み

①個人情報提供の要求

・サービス業者Ｂは、サービス業者Ａに対して個人データ提供を要求する。

②個人データ提供の同意要求

・サービス業者Ａは、情報主体に、サービス業者Ｂから個人データ提供の要求が来たことを通知する。

・このとき、サービス業者Ａは、サービス業者Ｂの少なくとも、以下の情報を情報主体に提供する。

【００７２】

サービス業者Ｂの名称、連絡先

個人データの利用目的

個人データを提供したときに受けられる特典、サービス

開示・訂正・削除請求の問い合わせ先と問い合わせ方法

サービス業者Ｂの身元を保証する電子証明書。例えば、サービス業者Ｂの保有するライセンスデータベースシステムの証明書など。

③提供の意思表示

・情報主体は、サービス業者Ａを通して、個人データをサービス業者Ｂへ提供するかどうかを決定する。

・提供する場合は、個人データ使用ライセンスを発行し、サービス業者Ａへ送信する。このとき、個人データ使用ライセンスは、サービス業者Ｂが保有しているライセンスデータベースシステムの公開鍵を用いて暗号化される。

【００７３】

このことにより、経由先のサービス業者Ａでは、個人データ使用ライセンスの使用はできない。

④暗号化個人データ取得

・サービス業者Ａは、情報主体から同意の通知がきた場合、サービス業者Ｂに暗号化個人データを送信する。

⑤ライセンス提供

・サービス業者Ｂは、サービス業者Ａから個人データ使用ライセンスを取得する。

【００７４】

図２２は、サービス業者Ｂへの個人データ使用ライセンスを発行するときのクライアントツールの処理を示すフローチャートである。

ステップＳ１１０において、サービス業者Ｂからの個人データ要求（サービス業者Ｂの証明書を含む）をサービス業者Ａから受信する。ステップＳ１１１において、情報主体は個人データを提供するか否かを判断する。ステップＳ１１１の判断がＮＯの場合には、ステップＳ１１２において、エラー処理を行い、処理を終了する。

【００７５】

ステップＳ１１１における判断がＹＥＳの場合には、ステップＳ１１３において、個人データを作成し、ステップＳ１１４において、共通鍵方式の鍵を生成する。そして、ステップＳ１１５において、個人データを暗号化し、ステップＳ１１６において、個人データ使用ライセンスを生成する。そして、ステップＳ１１７において、暗号化した個人データを送信する。そして、ステップＳ１１８において、ＤＲＭ認証する。ステップＳ１１８のＤＲＭ認証は、サービス業者Ｂの公開鍵を使用する。

【００７６】

ステップＳ１１８のＤＲＭ認証の結果が無効の場合には、ステップＳ１１９において、エラー処理を行い、処理を終了する。ステップＳ１１８のＤＲＭ認証の結果が有効である場合には、ステップＳ１２０において、個人データ使用ライセンスをサービス業者Ａへ送信して、処理を終了する。サービス業者Ａへ送られた個人データ使用ライセンスは、サービス業者Ｂに転送される。

３．１．１開示請求

図２３は、サービス業者間で個人データを取り引きする場合における、サービ

ス業者Ｂへの開示請求の処理を説明する図である。

【００７７】

情報主体がサービス業者Ｂに対して個人データの開示を請求するときに、サービス業者Ａを介してサービス業者Ｂに請求する。サービス業者Ａが情報主体とサービス業者Ｂの間にいる以外は、２．２節と同じ。

すなわち、

①サービス業者Ｂに対して、個人データの開示要求を出す。

②サービス業者Ａを介して、サービス業者Ｂに、情報主体へ個人データを開示するように要求する。

③サービス業者Ｂは、暗号化個人データとサービス業者Ｂが作成した付加情報を情報主体に送信する。

④情報主体は、受信した個人データを復号する。

３．１．２訂正請求

図２４は、サービス業者間で個人データを取り引きする場合における訂正請求の処理を説明する図である。

【００７８】

サービス業者Ａがサービス業者Ｂに個人データを提供している場合、情報主体からの個人データの訂正要求に応じる処理は、次のような流れである。

情報主体は、サービス業者Ａに訂正した暗号化個人データと訂正した使用ライセンスを送信する。サービス業者Ａは、訂正した個人データを同期するためにサービス業者Ｂに訂正情報を送信する。

【００７９】

すなわち、

①クライアントツールからサービス業者Ａに個人データ訂正要求が送られる。

②クライアントツールは、個人データを暗号化する。

③暗号化個人データがクライアントツールからサービス業者Ａへ送信される。

④サービス業者Ａでは、新しい個人データで古い個人データが更新され、暗号化個人データの同一性を保つための同期処理がサービス業者Ａからサービス業者Ｂに対して行われる。

⑤クライアントツールは、個人データ使用ライセンスをサービス業者Ａに提供する。サービス業者Ａでは、古い個人データ使用ライセンスが新しい個人データ使用ライセンスによって更新される。

⑥個人データ使用ライセンスの同一性を保つための同期処理がサービス業者Ａからサービス業者Ｂに対して行われる。

⑦サービス業者Ｂは、サービス業者Ａに訂正完了通知を送信する。

⑧サービス業者Ａは、情報主体に訂正完了通知を送信する。

【００８０】

図２５は、サービス業者間での個人データの同一性を保つための同期処理を示すフローチャートである。

ステップＳ１３０において、訂正請求の要求者へ訂正完了通知を送信する。ステップＳ１３１において、サービス業者Ａは、サービス業者Ｂへ訂正要求を送信する。ステップＳ１３２において、サービス業者Ａは、サービス業者Ｂから認証を受ける。ステップＳ１３２の認証の結果、無効と判断された場合には、ステップＳ１３３において、拒否通知をサービス業者Ａが受け取り、処理が終了する。ステップＳ１３２の認証の結果、有効と判断された場合には、ステップＳ１３４において、サービス業者Ａは、サービス業者Ｂへ訂正データを送信する。ステップＳ１３５において、サービス業者Ｂは、訂正データをＤＲＭ認証する。

【００８１】

ステップＳ１３５のＤＲＭ認証において、無効と判断された場合には、ステップＳ１３６において、エラー処理を行い、ステップＳ１３９において、要求拒否通知を受信し、処理を終了する。ステップＳ１３５において、ＤＲＭ認証の結果が有効の場合には、ステップＳ１３７において、訂正した個人データ使用ライセンスを送信し、ステップＳ１３８において、サービス業者Ｂからの訂正完了通知を受信して、処理を終了する。

３．１．３．削除請求

名簿を使用する場合における情報主体の個人データを削除する手順は、３．１．２節の訂正請求とほぼ同様である。異なるところは、訂正の場合は、訂正した情報に変更するが、削除の場合は、その処理はいらいないことである。

３．２．名簿を使用する場合

サービス業者Ａ、サービス業者Ｂともに個人データを、名簿を用いて使用する場合について、情報主体から、開示・訂正・削除請求に応じる流れを説明する。

３．２．１名簿を使用する場合の開示請求

３．１．１節と同じ。

３．２．２名簿を使用する場合の訂正請求

図２６は、名簿を使用する場合の訂正請求の処理を説明する図である。

【００８２】

サービス業者Ａがサービス業者Ｂに名簿を提供している場合、情報主体からの個人情報の訂正要求を応じる方法は、３．１．２節とほぼ同じである。

すなわち、情報主体から特定のサービス業者Ａ、Ｂへ個人データを提供している状況で、情報主体が個人データの修正を要求するとき、サービス業者Ａに対して、２つの個人データ使用ライセンスを発行する。個人データ使用ライセンスを発行するとき、情報主体は、サービス業者Ａのために、サービス業者Ａの公開鍵で暗号化した個人データライセンスと、サービス業者Ｂのために、サービス業者Ｂの公開鍵で暗号化した個人データ使用ライセンスをサービス業者Ａに送信する。受け取ったサービス業者Ａは、個人データ使用ライセンスをライセンスデータベースに保存し、ライセンスデータベースと名簿ライセンスデータベースを更新する。更に、サービス業者Ａは、サービス業者Ｂ用の個人データ使用ライセンスをサービス業者Ｂへ送信し、受け取ったサービス業者Ｂは、サービス業者Ａと同様に、名簿ライセンスデータベースを更新する。

【００８３】

図２７は、名簿を使用する場合の訂正要求におけるサービス業者Ａの処理のフローチャートである。

ステップＳ１５０において、訂正請求をしてきた要求者は登録者であるか否かの認証を行う。ステップＳ１５０の認証の結果、登録者でないと判断された場合には、ステップＳ１５１において、エラー処理を行い、ステップＳ１５２において、要求拒否通知を送信して処理を終了する。

【００８４】

ステップＳ１５０の認証の結果、要求者が登録者であると判断された場合には、ステップＳ１５３において、訂正データを要求する。そして、ステップＳ１５４において、訂正された暗号化データを受信し、ステップＳ１５５において、個人データ・データベースの更新を行い、ステップＳ１５６において、名簿データベースの更新を行う。

【００８５】

そして、ステップＳ１５７において、個人データ使用ライセンスのＤＲＭ認証を行う。ステップＳ１５７において、無効と判断された場合には、ステップＳ１５８において、エラー処理を行い、ステップＳ１５９において、要求拒否通知を送信して処理を終了する。

【００８６】

ステップＳ１５７のＤＲＭ認証において、有効と判断された場合には、ステップＳ１６０において、サービス業者Ａ、Ｂ用の使用ライセンスを受信する。そして、ステップＳ１６１において、ライセンスデータベースを更新し、ステップＳ１６２において、名簿ライセンスデータベースを更新する。ステップＳ１６３においては、サービス業者Ｂからサービス業者Ａが認証を受ける。ステップＳ１６３の認証が無効と判断された場合には、ステップＳ１６４において、エラー処理を行い、ステップＳ１６５において、要求拒否通知を受信し、処理を終了する。

【００８７】

ステップＳ１６３の認証が有効と判断された場合には、ステップＳ１６６において、訂正された暗号データをサービス業者Ｂに送信し、ステップＳ１６７において、サービス業者ＢによってＤＲＭ認証を受ける。ステップＳ１６７のＤＲＭ認証の結果が無効の場合には、ステップＳ１６８において、エラー処理を行い、ステップＳ１６９において、要求拒否通知を受信して処理を終了する。ステップＳ１６７のＤＲＭ認証の結果が有効の場合には、ステップＳ１７０において、サービス業者Ｂ用の個人データ使用ライセンスを送信して、処理を終了する。

３．２．３．名簿を使用する場合の削除請求

名簿を使用する場合における情報主体の個人データを削除する手順は、３．２．２節の訂正請求とほぼ同様である。異なるところは、訂正の場合は、訂正した

情報に変更するが、削除の場合は、その処理はいらないことである。すなわち、個人データと個人データ使用ライセンスを消去するだけである。

４．センタ型展開例

個人情報の提供を一手に引き受ける個人データ取り扱い事業者が、個人データセンタとなり、そのセンタが情報主体の個人データを管理し、サービス業者へ提供するという形態を考える。

【００８８】

ここでは、サービス業者は、個人データのリスト（名簿）の提供を望んでいるものとする。

この展開例においてはセンタは、サービス業者と情報主体との仲介をするだけである。具体的には、あるサービス業者からセンタに個人データ提供の要求があったときに、センタは、情報主体の個人データ使用ライセンスに従って、個人データを提供しても良いかを判断し、その結果、提供する場合は、提供した後に情報主体に通知する。

[ライセンスの提供の仕方]

センタは、様々なサービス業者からの個人データ提供要求を受け付けるが、そのたびに情報主体に使用同意を取っていたのでは、情報主体にとって利便性が悪い、また、センタはサービス業者に対して早急な対応ができない。

【００８９】

そこで、情報主体は、センタにライセンスを１００個あるいは１０００個といった、ある程度の数のライセンスを登録し、登録しておいたライセンスが無くなったときに、センタが、情報主体にライセンス登録の更新を要求する。

【００９０】

そして、センタがサービス業者に使用ライセンスを提供するときには、センタは、要求してきたサービス業者の業種や情報主体へのサービス内容、また、使用目的などが、情報主体が提供した使用ライセンス属性とマッチするかで判断をして提供する。

４．１センタ型展開例の概要

図２８は、センタ型個人データ提供システムの構成例である。

【００９１】

情報主体が、個人データ使用ライセンスを自ら発行する。ここでのセンタの役割は、主に、サービス業者からの提供要求の管理と、各情報主体が、どのサービス業者へ情報提供したかのデータを管理する。

【００９２】

この形態では、以下のような流れで個人情報が提供され使用される。

登録の流れ

１．情報主体は、センタに登録する。

・情報主体は、ある単位でライセンスをセンタに送信しておく。

２．センタは登録者に対して、ＩＤを発行する。

・センタは、サービス業者からの通知を送るために、登録者のＩＤと連絡先（電子メールアドレス）を対にしてリストにしておく。

提供の流れ

１．サービス業者は、センタに、ある条件（例えば、２０代の男性など）の個人情報（名簿）を提供するように要求する。

・このとき、サービス業者がセンタに提出するものは、「条件」と「事業者証明書」である。

２．センタは、登録者の中から条件に該当する情報主体を検索し、提供可能な情報主体を特定する。

３．２の該当者の個人データからなる名簿および名簿ライセンスを作成する。

４．センタは、暗号化名簿と名簿使用ライセンスをサービス業者に提供する。

５．サービス業者は、受け取った名簿を使用目的の範囲で名簿を使用する。

６．４の該当者に対してサービス業者に個人データを提供したことを通知する。そのとき、少なくともサービス業者の以下の情報を提供する。

・サービス業者の名称、連絡先

・個人情報の利用目的

・個人情報を提供したときに受けられる特典、サービスなど。

・開示・訂正・削除請求の問い合わせ先と問い合わせ方法。

４．１．１．該当する情報主体の検索方法について

センタがサービス業者からある条件の個人データの名簿を要求されたときに、センタは、以下の条件全てに満足する個人データを探す。この処理は、名簿ライセンスデータベースの検索ツールを使って実行される。

（１）サービス業者の業種

・サービス業者が提出する証明書に記載されている業種と情報主体が提出したライセンスの属性である提供許可業者を比較する。

【００９３】

例えば、Ｘ．５０９ｖ３証明書では、拡張領域に事業者の業種・サービス内容などを記述しておく。

Ｘ．５０９ｖ３証明書は、ＩＴＵ（International Telecomunications Union：国際電気通信連合電気通信標準化部門）が定めたデジタル証明書の標準仕様である。多くの場合、Ｘ．５０９ｖ３という書式に従う。ｖ３では拡張領域を設け、証明書発行者が独自の決められた情報を追加できるようにしている。

（２）サービス業者のサービスの提供内容

・サービス業者の証明書の情報とライセンスの属性である提供拒否サービスを比較する。

（３）サービス業者の個人データの使用目的

・サービス業者の使用目的とライセンスの属性である使用目的を比較する。

（４）サービス業者の要求している条件（３０歳未満でスポーツが趣味など）

・暗号化された名簿を復号し、サービス業者の提出した条件と個人データを比較する。

（１）、（２）に関しては、それらの情報を確かめるためにサービス業者の電子証明書の中に含め、正当性を検証できるようにする。

【００９４】

図２９は、検索ツール処理フローチャートを示す図である。

ステップＳ２００においては、サービス業者の証明書をロードする。ステップＳ２０１において、証明書の業種と合致する属性を持つ名簿ライセンスが存在するか否かを判断する。ステップＳ２０１における判断がＮＯの場合には、ステップＳ２０２において、エラー処理を行い、処理を終了する。ステップＳ２０１に

おける判断がＹＥＳの場合には、ステップＳ２０３において、合致するライセンスを残す。そして、ステップＳ２０４において、証明書にあるサービスと合致する属性を持つ名簿ライセンスが存在するか否かを判断する。ステップＳ２０４の判断がＮＯの場合には、ステップＳ２０４ａにおいて、エラー処理を行い、処理を終了する。ステップＳ２０４における判断がＹＥＳの場合には、ステップＳ２０５において、合致するライセンスを残す。ステップＳ２０６においては、サービス業者の要求する使用目的と合致する属性を持つ名簿ライセンスが存在するか否かを判断する。ステップＳ２０６の判断がＮＯの場合には、ステップＳ２０６ａにおいてエラー処理を行い、処理を終了する。

【００９５】

ステップＳ２０６の判断において、ＹＥＳと判断された場合には、ステップＳ２０７において、合致するライセンスを残し、ライセンス－名簿ＩＤを取得する。ステップＳ２０８において、対応する暗号化された名簿をロードし、ステップＳ２０９において、名簿を復号し、ステップＳ２１０において、現在残っているライセンスに対応する個人データを残す。そして、ステップＳ２１１において、サービス業者の要求する条件を満たす個人データが存在するか否かを判断する。

【００９６】

ステップＳ２１１における判断がＮＯの場合には、ステップＳ２１２において、エラー処理を行い、処理を終了する。ステップＳ２１１にける判断がＹＥＳの場合には、ステップＳ２１３において、合致する個人データを残し、ステップＳ２１４において、残った個人データのＩＤと使用した名簿のライセンス－名簿ＩＤを取得し、処理を終了する。

【００９７】

以上において、ステップＳ２００からステップＳ２０７は、ライセンスとサービス業者の証明書だけで行う処理であり、ステップＳ２０８からステップＳ２１４は、復号された個人データとサービス業者の要求条件で行う処理である。

４．２センタへの登録

図３０は、センタへの登録処理を説明する図である。

①個人情報の運用に関する事項の通知

・個人情報センタは、情報主体に個人情報を登録してもらう際、必ず個人情報の運用についての規定を提示する。

・その内容については、必ず以下の事柄を含んでいる。

（ア）第三者へ提供することが、利用目的であること

（イ）第三者への提供手段・方法

（ウ）情報主体の求めに応じて、開示・訂正・削除ができること

（エ）情報主体の求めに応じて、このサービスの停止ができ、かつ個人情報センタの登録簿からその情報主体の情報が削除されること

（オ）登録するときに、必要な個人情報の項目

・登録フォームも含まれている。情報主体は、このフォームに個人情報を入力する。

②フォーム要求

・情報主体が上記の内容を吟味した上で、登録したいと思ったら、個人情報センタへ登録フォームを要求する。

③フォームの提供

・個人情報主体は、フォームの要求を受けたら、登録フォームを送信する。

④個人情報の暗号化

・情報主体は、登録フォームに個人情報を入力し、フォームを暗号化するクライアントツールを使用して共通鍵暗号方式の鍵を生成し、その鍵で暗号化する。

⑤個人情報の登録

・暗号化した個人情報を個人情報センタに提供する。

⑥登録者のリストを作成

・個人データ管理ツールは、登録者に登録者識別子（ＩＤ）を発行し、そのＩＤと電子メールアドレスを対にしたリストを作成する。

・このリストは、各登録した情報主体と、その情報主体が個人情報を提供したサービス業者の情報を関連付けたリストとなる。表３参照。

【００９８】

【表３】

| 業者名 | 業種 | サービス内容 | 住所 | 問い合わせ先 | 提供項目 | 利用目的 |
|---|---|---|---|---|---|---|
| ○○株式会社 | メーカー | --- | ○○○○○ | ○○－□□□ | 氏名/性別/生年月日/住所/メールアドレス/興味のある分野/ | 市場調査/ |
| △△△ | 情報処理 | --- | △△△△△ | ○○－△△△ | 氏名/性別/生年月日/趣味 | 市場調査/ |
| ・<br>・<br>・ | ・<br>・<br>・ | ・<br>・<br>・ | ・<br>・<br>・ | ・<br>・<br>・ | ・<br>・<br>・ | ・<br>・<br>・ |
| ××保険 | 金融 | --- | ××××××× | ○○－××× | 氏名/性別/生年月日/住所/収入/ | 広告 |

【００９９】

・このリストは、サービス業者から要求があった場合に、登録者（情報主体）に通知するために用いられる。また、登録者から開示・訂正・削除請求をするため、その人が、どのサービス業者に情報を提供しているかを確認する目的で使用される。

⑦ライセンスを提供

・情報主体は、暗号化個人情報と、センタ側でサービス業者が要求する条件の個人データを検索するための検索用ライセンスとある単位の使用ライセンスを登録する。

なお、⑦の個人データ管理ツールとは、以下のようなもの。

［個人データ管理ツール］

個人情報取扱事業者が、個人データを第三者に提供するとき、個人情報取扱事業者は、表３のような情報主体別に、その情報主体の個人情報をどの事業者に提供したかの一覧を管理する。個人データ管理ツールとは、このような情報主体別にその個人情報を提供した事業者のリストを生成するツールのことである。また、このツールは、情報主体の個人情報を一切使用しないので、ＤＲＭ機能は必要ない。

４．３個人データの提供

図３１は、個人データの提供処理を説明する図である。

①個人情報提供要求

・サービス業者は個人情報センタへ個人情報名簿の提供を要求する。

・具体的には、サービス業者は２０代の男性などある条件の名簿を要求する。

・サービス業者の（業種・サービス内容などの企業情報の）証明書を提出する。

②該当者を検索

・個人情報センタは、検索ツールを用いて、サービス業者が要求している該当の情報主体を１．１．１節の方法で検索する。

・検索ツールは、暗号化個人情報と検索用ライセンスとサービス業者の要求条件と事業者証明書が入力され、該当のＩＤのリストが出力される。

③名簿を作成する

・個人情報センタは、第三者提供に対し、名簿作成ツールを使用して、②に該当する情報主体の個人情報からなる暗号化名簿とその名簿の使用ライセンスを作成し、各々名簿データベースシステム、名簿使用ライセンスデータベースシステムに保存する。

④名簿の提供

・個人情報センタは、暗号化名簿と名簿ライセンスをサービス業者へ提供する。

⑤提供先リストを更新する

・個人データ管理ツールは、③で作成された名簿に載っている情報主体に対して提供先リストの更新をする。

⑥提供通知

・個人情報センタは、各情報主体に対してサービス業者へ個人情報を提供したことを通知する。

・このとき、センタは、サービス業者に関する少なくとも以下の情報を通知する。

【０１００】

サービス業者の名称、連絡先

個人情報の利用目的

個人情報を提供したときにうけられる特典、サービスなど。

【０１０１】

開示・訂正・削除請求の問い合わせ先と問い合わせ方法。

図３２は、センタの提供処理フローチャートである。

ステップＳ２２０において、サービス業者の証明書の検証を行う。ステップＳ

２２１において、無効と判断された場合には、ステップＳ２２２において、エラー処理を行い、処理を終了する。ステップＳ２２１において、有効と判断された場合には、ステップＳ２２３において、検索ツールで該当者を検索する。ステップＳ２２３において、該当者がいないと判断された場合には、ステップＳ２２４において、サービス業者に通知し、処理を終了する。ステップＳ２２３において、該当者がいると判断された場合には、ステップＳ２２５において、名簿作成ツールで名簿と名簿使用ライセンスを作成する。そして、ステップＳ２２６において、名簿と名簿使用ライセンスをデータベースに保存し、ステップＳ２２７において、作成した暗号化された名簿のコピーをサービス業者に送信する。そして、ステップＳ２２８において、ＤＲＭ認証し、ステップＳ２２８のＤＲＭ認証が無効の場合には、ステップＳ２２９において、エラー処理して処理を終了する。ステップＳ２２８のＤＲＭ認証が有効と判断された場合には、ステップＳ２３０において、作成した名簿ライセンスを送信し、ステップＳ２３１において、作成した名簿に載っている情報主体の提供先リストを更新する。そして、ステップＳ２３２において、情報主体に提供したことを通知して、処理を終了する。

【０１０２】

図３３は、名簿作成ツールのフローチャートである。

ステップＳ２５０において、検索ツールから該当のライセンス－名簿ＩＤと個人データＩＤを取得する。ステップＳ２５１において、名簿データベースへ該当の暗号化名簿をロードする。ステップＳ２５２において、暗号化名簿を作成し、ステップＳ２５３において、作成された暗号化名簿を名簿データベースに保存する。そして、ステップＳ２５４において、名簿ライセンスを作成して、処理を終了する。

【０１０３】

図３４は、提供される名簿ライセンスの作成の概略を示す図である。名簿ライセンスデータベースに保存されているデータから所定の条件を満たすデータのみを取り出し、データが取り出された後の名簿ライセンスとデータを取り出して作った名簿ライセンスとができる。データを取り出して作った名簿ライセンスは、名簿作成ツールで作成され、ユーザに提供される。

４．４開示請求

開示請求は、基本的には、暗号化個人データとそれに付随する情報を情報主体に送信することなので、２．２節及び３．１．１節と同じようになる。

【０１０４】

ただし、センタ型モデルの場合は、個人情報管理ツールが作成したリストを暗号化個人データと一緒に情報主体に提供する。

４．５訂正請求

図３５は、訂正請求の処理の流れを説明した図である。

【０１０５】

情報主体は、個人データを個人データセンタとサービス業者に渡しているが、いずれにしても情報主体は、センタに訂正要求すれば、提供した全てのサービス業者に訂正が反映される。

（１）訂正要求

・情報主体は、個人情報センタに個人情報の訂正を要求する。

（２）訂正した暗号化個人データを送信

・情報主体は、訂正した個人データを暗号化し、その暗号化個人データを個人情報センタに送信する。個人データの暗号化に関しては、訂正する項目について新たに共通鍵暗号方式の暗号化鍵を生成し、それを使用する。

（３）個人データの訂正

・センタは、個人情報データベースにある情報主体の古い個人データを削除し、新しい暗号化個人データに更新する。

（４）訂正すべき名簿の検索

・訂正を要求した情報主体が関係している名簿を個人データ管理ツールで検索する。

（５）名簿の訂正

・名簿作成ツールを用いて暗号化名簿を作成し直し、更新された暗号化名簿を名簿データベースシステムに保存する。

（６）暗号化個人データの同期

・サービス業者は、訂正した暗号化名簿をサービス業者の名簿データベースシス

テムと同期するために、訂正した暗号化名簿を送信する。

（７）訂正したライセンスを送信

・情報主体は、（２）で使用した暗号鍵をライセンスの中に入れ、新しい使用ライセンスを作成し、ライセンスをセンタへ送信する。

（８）ライセンスの訂正

・センタは、ライセンスデータベースシステムの中で、古い情報主体のライセンスを削除し、受け取った使用ライセンスに更新する。

（９）名簿ライセンスの訂正

・名簿作成ツールを用いて名簿ライセンスを作成し直し、更新された名簿ライセンスを名簿ライセンスデータベースシステムに保存する。

（１０）名簿ライセンスの同期

・サービス業者は、訂正した名簿ライセンスをサービス業者の名簿ライセンスデータベースシステムと同期するために、訂正した名簿ライセンスを送信する。

（１１）訂正完了通知

・個人情報センタは、訂正が完了したことを情報主体に通知する。

【０１０６】

図３６は、名簿使用時のサービス業者の訂正同期処理フローチャートである。

ステップＳ２６０において、要求者へ訂正完了通知送信がされ、ステップＳ３２６１において、訂正した名簿を使用している事業者は存在するか否かが判断される。ステップＳ２６１において、存在しないと判断された場合には処理を終了する。ステップＳ２６１において、存在すると判断された場合には、ステップＳ２６２において、事業者へ訂正要求を送信し、ステップＳ２６３において、サービス事業者からユーザ認証を行う。ステップＳ２６３の結果、無効の場合には、ステップＳ２６４において、拒否通知が受信され、処理を終了する。

【０１０７】

ステップＳ２６３の結果、有効と判断された場合には、サービス業者へ訂正データを送信し、ステップＳ２６６において、ＤＲＭ認証する。ステップＳ２６６のＤＲＭ認証の結果が無効の場合には、ステップＳ２６７において、エラー処理を行い、ステップＳ２６８において、要求拒否通知の受信が行われ、処理を終了

する。ステップＳ２６６において、ＤＲＭ認証の結果、有効と判断された場合には、ステップＳ２６９において、訂正した使用ライセンスを送信し、ステップＳ２７０において、事業者からの訂正完了通知を受信し、ステップＳ２７１において、訂正した名簿を使用している事業者は存在するか否かを判断する。ステップＳ２７１において、ＮＯと判断された場合には、処理を終了するが、ＹＥＳと判断された場合には、ステップＳ２６２に戻る。

４．６．削除請求

情報主体からの削除要求には、次の２つがある。

（１）サービス業者が保持している名簿から個人データを削除する。

（２）個人情報センタが保持しているデータベースから削除する。これは、センタからのサービスの停止である。

４．６．１．サービス業者の中のデータの削除

図３７は、サービス業者が有する個人データの削除処理を説明する図である。

【０１０８】

情報主体が、あるサービス業者だけからサービスを停止する場合の流れを以下に示す。

①削除要求

・情報主体は、特定のサービス業者Ａに対して個人データの削除を要求する。

②削除要求通知

・個人情報センタは、サービス業者Ａに情報主体から削除を要求されていることを通知する。

③名簿／名簿ライセンスの訂正

・個人情報センタは、名簿作成ツールを用いて、サービス業者Ａに提供している名簿と名簿ライセンスを訂正する。

・具体的には、サービス業者に提供している暗号化された名簿から要求している情報主体の個人データを削除し、名簿ライセンスからその情報主体の使用ライセンス鍵を削除し、名簿ライセンスを更新する。

④訂正した名簿を送信する

・さーびす業者Ａは、これまで使用していた名簿を名簿データベースから削除し

、訂正された名簿を名簿データベースに保存する。

⑤訂正した名簿ライセンスを送信する。

・サービス業者Ａは、これまで使用していた名簿ライセンスを名簿ライセンスデータベースから削除し、訂正された名簿ライセンスを名簿ライセンスデータベースに保存する。

⑥削除完了通知

・個人情報センタは、情報主体にすべての処理が終わったことを通知する。

４．６．２．センタの有する個人データの削除

図３８は、センタの有する個人データの削除処理を説明する図である。

【０１０９】

個人情報センタの提供要求通知サービスを停止する流れを以下に示す。

①削除要求

・情報主体は、センタに個人情報の削除（センタからのサービスの停止）を要求する。

②暗号化個人データの削除

・個人情報センタは、要求している情報主体の暗号化個人データを削除する。

③使用ライセンス削除

・個人情報センタは、要求している情報主体の使用ライセンスを削除する。

④訂正すべき名簿の検索

・個人情報センタは、個人データ管理ツールを用いて、要求している情報主体に関係する名簿を検索する。

⑤訂正すべき名簿とそのライセンスを収集

⑥名簿／名簿ライセンスの訂正

・個人情報センタは、名簿作成ツールを用いて名簿と名簿ライセンスを訂正する。

・具体的には、名簿から要求している情報主体の情報を削除し、名簿ライセンスに含まれている情報主体の鍵も削除する。

⑦訂正した名簿を送信する

・個人情報センタは、訂正した名簿をサービス業者へ送信し、サービス業者は、

名簿データベースシステムにある以前の名簿を削除し、訂正された名簿に更新する。

⑧訂正した名簿ライセンスを送信する

・個人情報センタは、訂正した名簿ライセンスをサービス業者へ送信し、サービス業者は、名簿ライセンスデータベースシステムにある以前の名簿ライセンスを削除し、訂正された名簿ライセンスに更新する。

⑨削除完了通知

・個人情報センタは、情報主体に全ての処理が終わったことを通知する。

４．７センタ型におけるビジネスの一形態

図３９は、センタ型ビジネスの一形態における情報主体、センタ、業者の関係を示す図である。

【０１１０】

個人情報センタが中心となり情報主体、サービス業者にサービスを提供するビジネス形態を考える。

４．７．１情報主体と個人情報センタの関係

・情報主体は、センタに個人情報を提供する。

・センタは、情報主体が登録する際にポイントを与える。

・センタは、サービス業者に個人データを提供するときにポイントを与える。

・情報主体は、ある程度ポイントが貯まったら、商品および現金と交換できる。

[ポイントの加算方法について]

センタは、登録している情報主体に対して以下の時にポイントを加算する。

・情報主体が個人情報センタに個人データを登録するとき。

【０１１１】

・個人データを提供するとき、情報主体は、暗号化個人データとその使用ライセンスを提供する。使用ライセンスは、情報主体しか発行できないので最初に１００個なり１０００個なりを提供しておく。

【０１１２】

・センタは、ライセンスがなくなったとき、情報主体にライセンスの発行を要求する。

・センタが個人データをサービス業者に提供するとき

なお、ポイントの加算方法などは、例えば、表４のように設定する。

【０１１３】

【表４】

| | | ポイント（情報主体向け） | 料金（事業者向け） |
|---|---|---|---|
| 使用期限 | | 100 ポイント/半年 | 1000 円/半年 |
| 移動回数 | | 10 ポイント/移動回数 | 100 円/移動回数 |
| 使用目的 | 調査 | 5 ポイント | 50 円 |
| | 貸与・販売 | 10 ポイント | 100 円 |
| | マイニング | 7 ポイント | 70 円 |
| | ・<br>・<br>・ | ・<br>・<br>・ | ・<br>・<br>・ |

【０１１４】

４．７．２センタとサービス業者の関係

・センタは個人データをサービス業者へ提供する。

・サービス業者は、センタに個人データの使用料金を支払う。

【０１１５】

サービス業者から名簿提供の要求がきたときに、個人情報センタは、暗号化名簿と名簿使用ライセンスを提供する。そのとき、個人情報センタは、サービス業者の名簿の使用に対して料金を徴収する。ただし、実際には、暗号化名簿は、一旦名簿データベース上に保存されればよいので、サービス業者は、初めてセンタに名簿を要求するときにだけ提供される。したがって、その後のサービス業者からの名簿要求は、名簿ライセンスだけになる。ただし、情報主体からセンタへ個人データの訂正があった場合、センタは、個人データの同期をするために個人データベースを送信することがある。

【０１１６】

個人情報センタは、ライセンスをサービス業者へ提供するとき、ライセンス料計算装置と課金システムによりライセンス使用金額が計算される。ライセンス価値計算装置とは、発行された使用ライセンスを数値（金額やポイント）に変換す

る装置である。課金システムは、金額データを集計して請求金額を計算するシステムである。

４．７．３情報主体とサービス業者

・サービス業者は、情報主体にサービスを提供する

・情報主体は、サービス業者にサービス料金を支払う。

４．７．４ライセンスの価格設定について

ライセンスは、その利用条件によりポイント・金額が変わると考えた方が自然である。例えば、同じ暗号化個人データに関して、その使用ライセンスの期限属性が１日と１ヶ月とを比べた場合、やはり１ヶ月の使用ライセンスの方が価値が高いと考えられる。このような使用ライセンスの使用条件による値段の価値基準は、予め個人情報センタが定めるか、あるいはサービス業者とセンタが話し合いなどして決定する。例えば、表４のようなポイント及び料金体系を定める。ただし、料金・ポイントは、センシティブな個人データになれば、当然ポイント・料金体系も変化する。

４．７．５ビジネス形態の処理の流れ

データの流れ

図４０は、データの流れを示す図である。

【０１１７】

個人情報センタ、サービス業者は、すでに暗号化個人データを保有していると仮定し、情報主体は、センタが提供するサービスに登録していると仮定する。このときの情報主体からセンタを通じサービス業者までの一連のデータの流れを以下に示す。

①ライセンスの送信

・情報主体は、センタに登録する際、使用ライセンスを送信する。

②ライセンスの価値をポイントに換算

・センタのライセンス料計算装置により、受信した使用ライセンスが何ポイントになるか計算する。

③ポイント加算

・②で計算したポイントをポイントデータベースの累積ポイントと加算し、ポイ

ントを更新する。

④ライセンス提供

・センタは、要求のあったサービス業者へ使用ライセンスを送信する。

・ライセンスデータベースシステムにライセンスの送受があった場合、トランザクションデータベースに記録される。

⑤ライセンスの価値を料金に換算

・センタのライセンス料計算装置により、送信した使用ライセンスのポイント数と料金を計算する。このポイント数は、その情報主体の累積ポイントに加算される。

・サービス業者のライセンス料計算装置により、受信した使用ライセンスの料金を計算する。

⑥料金加算

・⑤で計算された料金は、センタ、サービス業者各々の課金システムに加算される。

⑦料金集計

・センタの課金システムは、金額データを集計して請求金額を計算する。

⑧料金の請求

・課金システムは、センタが契約している銀行に料金を請求する。

【０１１８】

（付記１）暗号化された個人データを受信するステップと、

暗号化された、該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを受信するステップと、

前記復号鍵と個人データ使用ライセンスを復号するステップと、

前記個人データの用途が前記個人データ使用ライセンスに記述された使用条件と一致するかを判断するステップと、

前記個人データの用途が前記使用条件と一致するときのみに前記復号された復号鍵を用いて前記個人データを復号するステップとを有することを特徴とする個人データ保護流通方法。

【０１１９】

（付記２）前記復号鍵と個人データ使用ライセンスはＤＲＭ認証技術を用いて暗号化及び復号化されることを特徴とする付記１に記載の個人データ保護流通方法。

【０１２０】

（付記３）前記個人データ使用ライセンスをＤＲＭ認証技術を用いて復号化するための機構は、ＴＲＭ化されていることを特徴とする付記２に記載の個人データ保護流通方法。

【０１２１】

（付記４）前記個人データ使用ライセンスの使用条件には、該個人データ使用ライセンスの有効期限、使用可能回数、使用目的、移動回数のいずれかを少なくとも含むことを特徴とする付記１に記載の個人データ保護流通方法。

【０１２２】

（付記５）前記使用目的は、前記個人データを使用するアプリケーションの限定を含むことを特徴とする付記４に記載の個人データ保護流通方法。

（付記６）前記暗号化された個人データ及び該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを複数の情報主体より受信するステップと、

複数の前記個人データ使用ライセンスを同一な条件の単位で連結して名簿ライセンスを作成するステップと、

該名簿ライセンスの作成に使用された個人データ使用ライセンスに対応する、暗号化された個人データを連結して名簿を作成するステップを有することを特徴とする付記１に記載の個人データ保護流通方法。

【０１２３】

（付記７）前記暗号化された個人データは該個人データを送信した情報主体が有する復号鍵によって復号可能となっていることを特徴とする付記６に記載の個人データ保護流通方法。

【０１２４】

（付記８）前記個人データを他の情報装置に提供する場合には、前記個人データの情報主体ごとに提供した他の情報装置を管理する組織の名称、業種、使用

目的、問い合わせ先、提供した個人データベースの項目リストのうち少なくとも一つを作成し、必要に応じて対応する情報主体に開示することを特徴とする付記６に記載の個人データ保護流通方法。

【０１２５】

（付記９）前記暗号化された個人データ及び該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスの少なくとも一つに訂正がある場合に、前記訂正された内容を受信するステップと、

該訂正された内容を他の情報装置に送信して、個人データ及び個人データ使用ライセンスの同一性を確保するステップとを有することを特徴とする付記８に記載の個人データ保護流通方法。

【０１２６】

（付記１０）暗号化された個人データを受信するステップと、

暗号化された、該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを受信するステップと、

前記復号鍵と個人データ使用ライセンスを復号するステップと、

前記個人データの用途が前記個人データ使用ライセンスに記述された使用条件と一致するかを判断するステップと、

前記個人データの用途が前記使用条件と一致するときのみに前記復号された復号鍵を用いて前記個人データを復号するステップとをコンピュータに実行させることを特徴とする個人データ保護流通プログラム。

【０１２７】

（付記１１）暗号化された個人データを受信する手段と、

暗号化された、該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを受信する手段と、

前記復号鍵と個人データ使用ライセンスを復号する手段と、

前記個人データの用途が前記個人データ使用ライセンスに記述された使用条件と一致するかを判断する手段と、

前記個人データの用途が前記使用条件と一致するときのみに前記復号された復号鍵を用いて前記個人データを復号する手段とを有することを特徴とする個人デ

ータ保護流通装置。

【０１２８】

【発明の効果】

本発明によれば、社内での個人情報管理規定について詳細に決めていなくても、（少なくとも特定の従業員だけが、個人データ・データベースへのアクセス権を持つようにすることは必要であるが）個人データは、不正の使用、目的外使用から保護される。

【０１２９】

情報主体は、提供する個人データ取扱事業者が世間一般に特別信頼されていなくても、本発明によれば、サーバ装置を設置して有れば、安心して個人データを提供することができる。

【図面の簡単な説明】

【図１】

情報主体、事業者、第三者の関係を説明する図である。

【図２】

本発明の実施形態の構成の概略構成を説明する図である。

【図３】

情報主体が個人情報を提供することに同意した場合の提供の仕組みと、サービス業者がその情報を利用する仕組みを示す図である。

【図４】

使用条件と個人データの使用との関係を説明する図である。

【図５】

ＤＲＭ認証を説明する図である。

【図６】

クライアントツールの個人データ使用ライセンスの送信時のフローチャートである。

【図７】

個人データと個人データ使用ライセンスとの関係を説明する図である。

【図８】

アプリケーションで個人データを使用する際のフローチャートである。

【図９】

ライセンスデータベースシステムのライセンス送信時のフローチャートである。

【図１０】

本発明の実施形態の別の構成における適用例を説明する図である。

【図１１】

情報主体から開示請求があった場合の開示の仕組みを示す図である。

【図１２】

情報主体からの個人データの訂正請求における動作を説明する図である。

【図１３】

サービス業者側の個人データの訂正処理のフローチャートである。

【図１４】

ライセンス代理提供サーバによる個人データの削除処理を説明する図である。

【図１５】

名簿ライセンスの生成処理を説明する図である。

【図１６】

名簿の作成と名簿ライセンスの生成処理を図示した模式図である。

【図１７】

名簿作成ツールが名簿・名簿ライセンスを作成する処理のフローチャートである。

【図１８】

名簿の使用形態を説明する図である。

【図１９】

名簿使用時の訂正要求の処理を説明する図である。

【図２０】

名簿使用時のサービス業者の名簿の訂正処理を示すフローチャートである。

【図２１】

サービス業者間で個人データを取り引きする処理を示す図である。

【図２２】

サービス業者Ｂへの個人データ使用ライセンスを発行するときのクライアントツールの処理を示すフローチャートである。

【図２３】

サービス業者間で個人データを取り引きする場合における、サービス業者Ｂへの開示請求の処理を説明する図である。

【図２４】

サービス業者間で個人データを取り引きする場合における訂正請求の処理を説明する図である。

【図２５】

サービス業者間での個人データの同一性を保つための同期処理を示すフローチャートである。

【図２６】

名簿を使用する場合の訂正請求の処理を説明する図である。

【図２７】

名簿を使用する場合の訂正要求におけるサービス業者Ａの処理のフローチャートである。

【図２８】

センタ型個人データ提供システムの構成例である。

【図２９】

検索ツール処理フローチャートを示す図である。

【図３０】

センタへの登録処理を説明する図である。

【図３１】

個人データの提供処理を説明する図である。

【図３２】

センタの提供処理フローチャートである。

【図３３】

名簿作成ツールのフローチャートである。

【図３４】

提供される名簿ライセンスの作成の概略を示す図である。

【図３５】

訂正請求の処理の流れを説明した図である。

【図３６】

名簿使用時のサービス業者の訂正同期処理フローチャートである。

【図３７】

サービス業者が有する個人データの削除処理を説明する図である。

【図３８】

センタの有する個人データの削除処理を説明する図である。

【図３９】

センタ型ビジネスの一形態における情報主体、センタ、業者の関係を示す図である。

【図４０】

データの流れを示す図である。

【符号の説明】

１０　　個人データ

１１　　復号鍵

１２　　個人データ使用ライセンス

１３、１５　　セッション鍵

１４　　公開鍵暗号方式の鍵

２０　　情報主体／クライアントツール

２１　　サービス業者のコンピュータ

２２　　個人データ・データベースシステム

２３　　ライセンスデータベースシステム

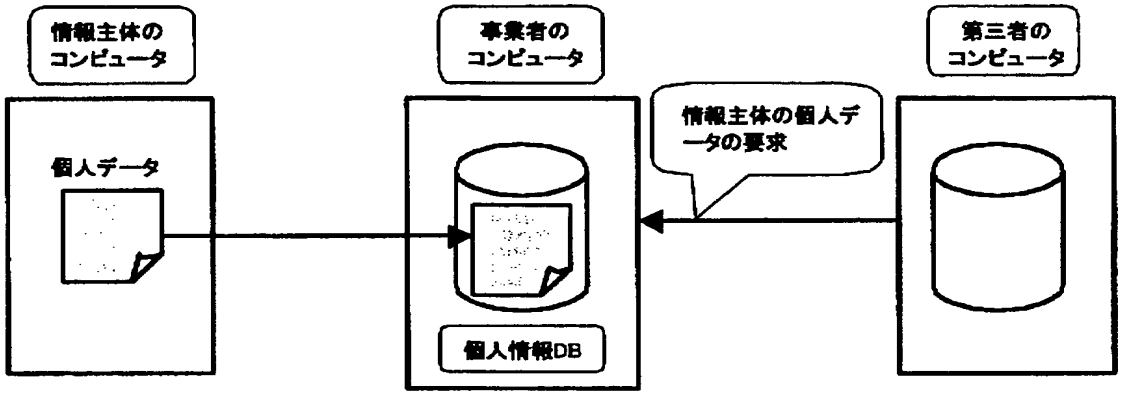
２４　　アプリケーション

２５　　ネットワーク

【書類名】　　図面

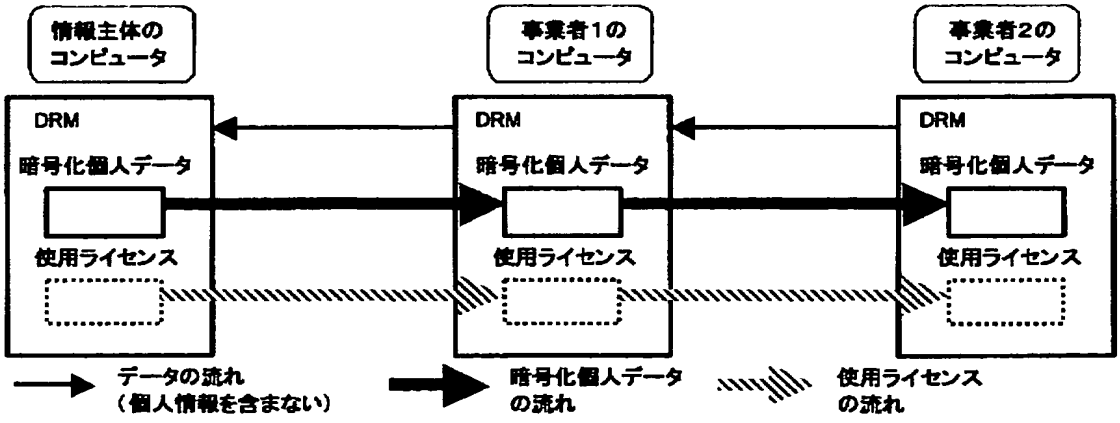
【図１】

情報主体、事業者、第三者の関係を説明する図



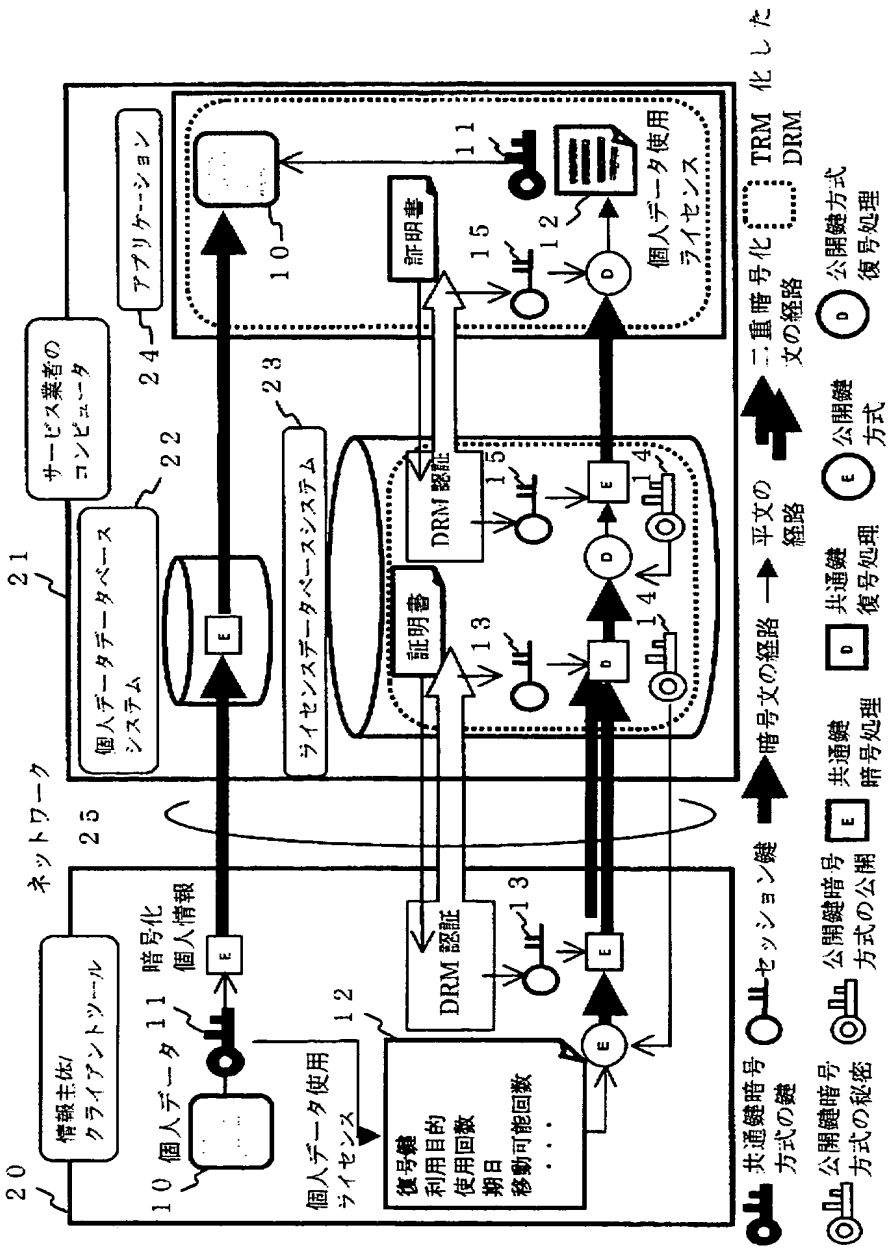

【図２】

本発明の実施形態の構成の概略構成を説明する図



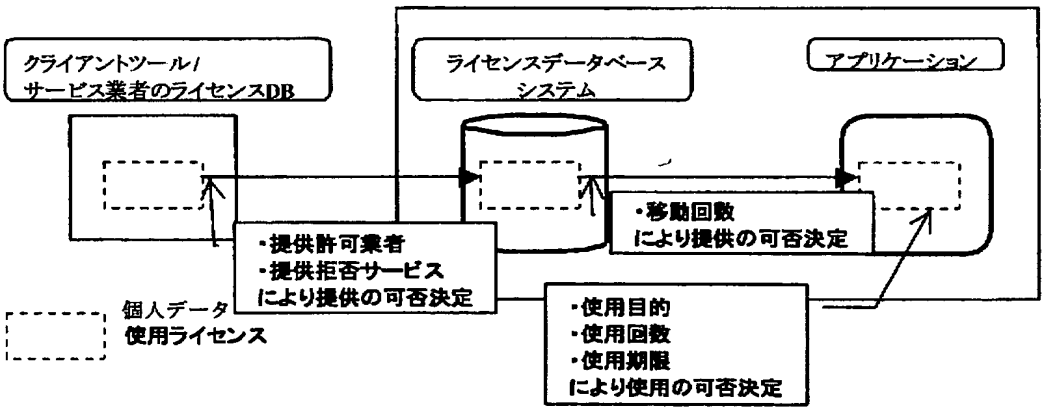
【図３】

**情報主体が個人情報を提供することに同意した場合の提供の仕組みと、サービス業者がその情報を利用する仕組みを示す図**



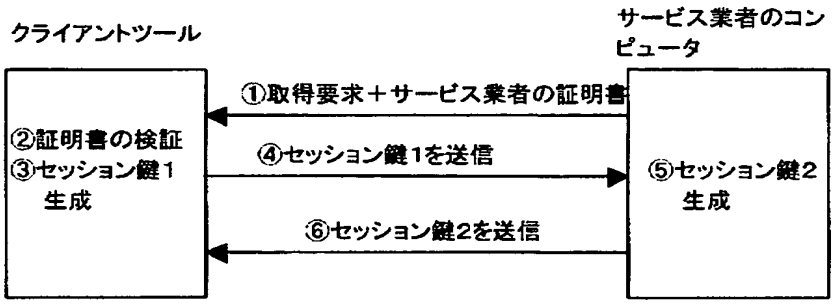
【図４】

使用条件と個人データの使用との関係を説明する図



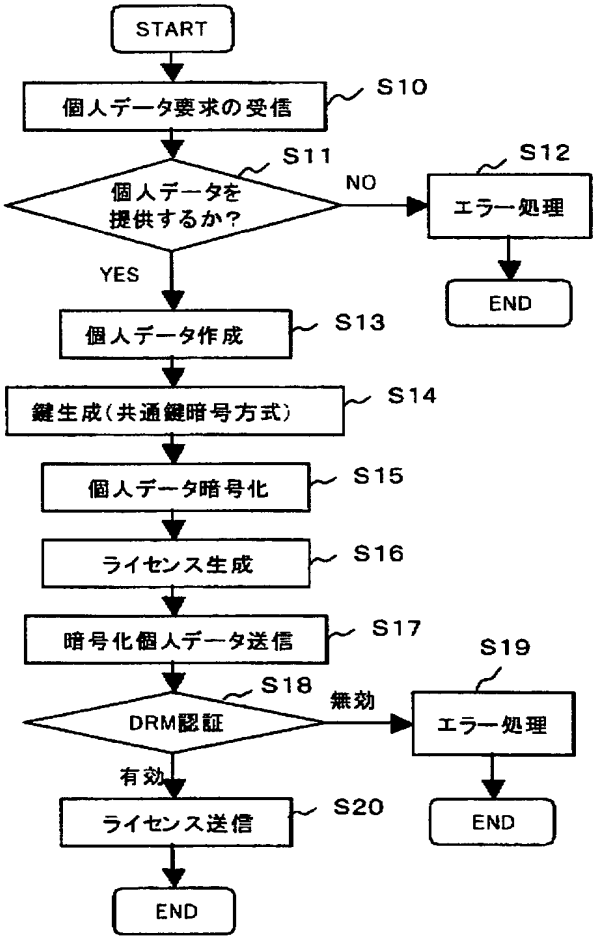

【図５】

DRM認証を説明する図



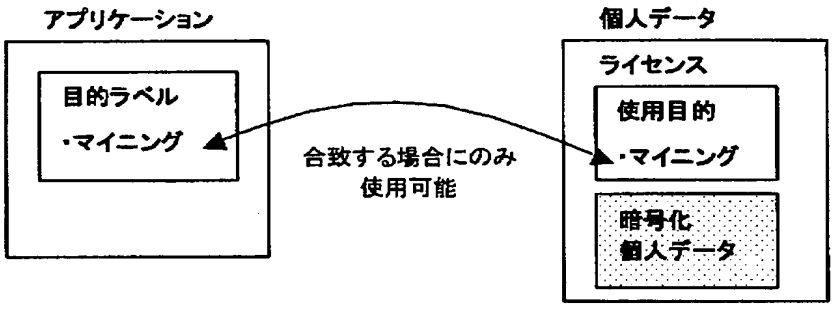
【図６】

情報主体のコンピュータにおいてクライアントツールの
個人データ使用ライセンスの送信時のフローチャート



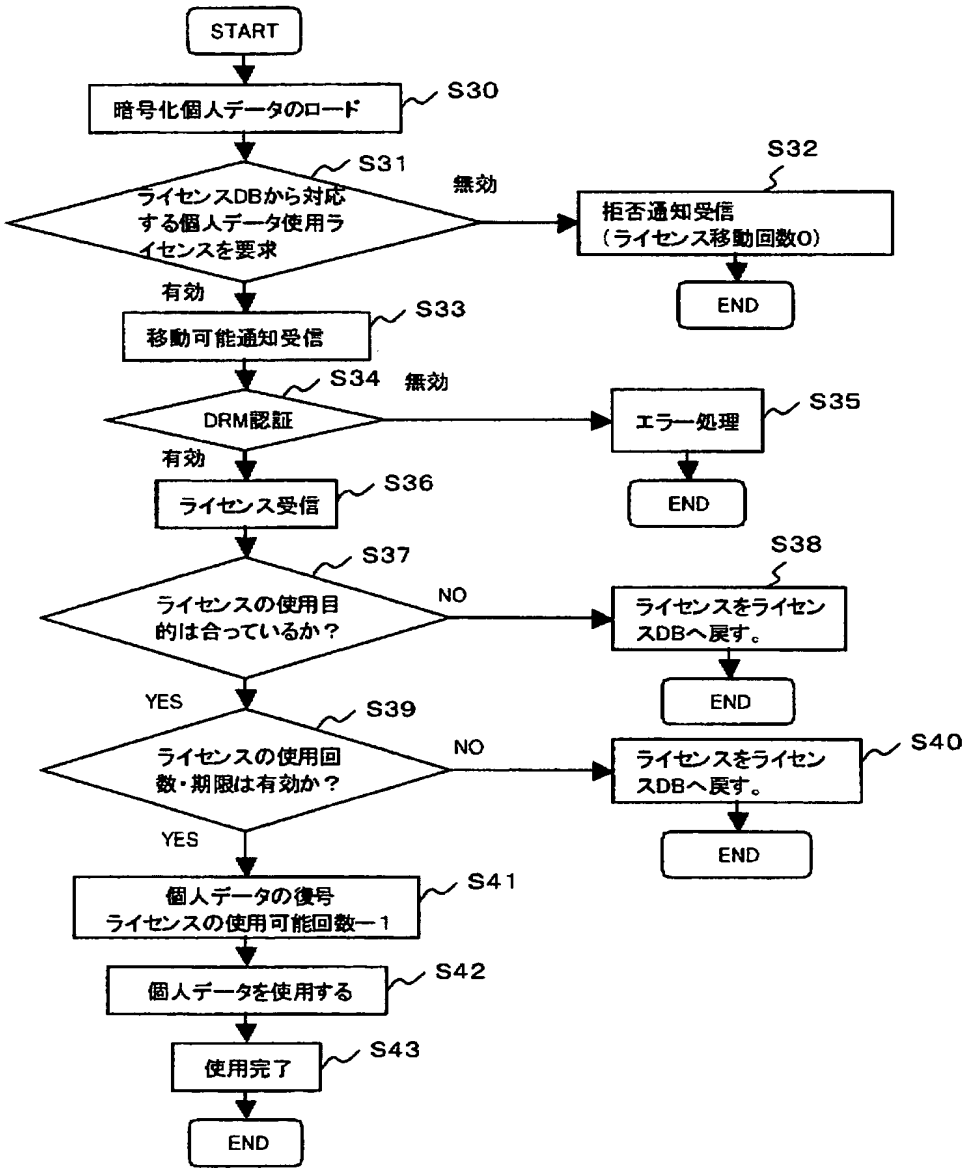
【図７】

# 個人データと個人データ使用ライセンスとの関係を説明する図



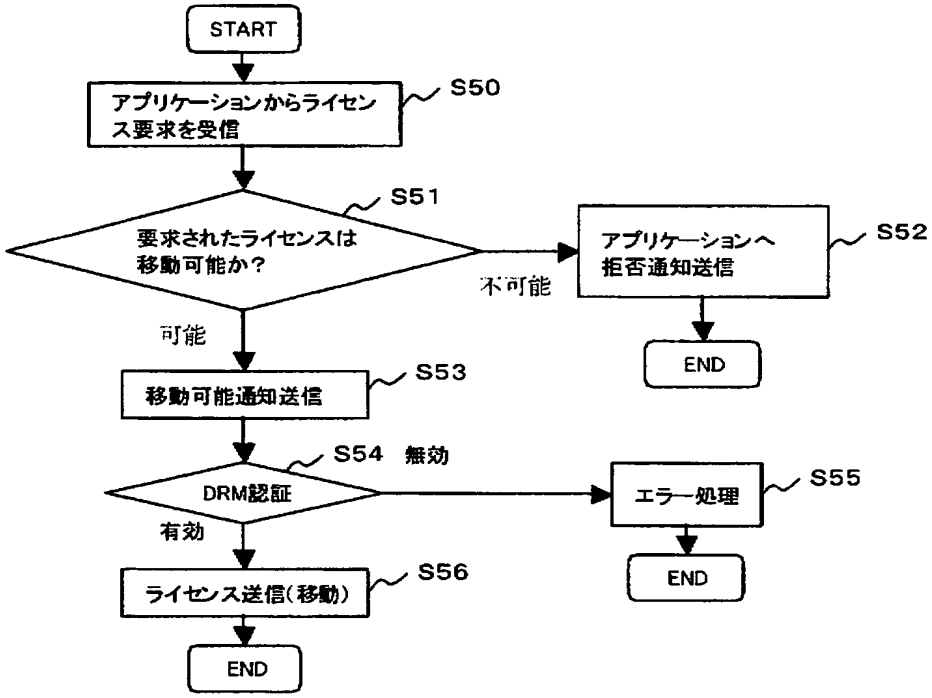
【図８】

サービス業者のアプリケーションで
個人データを使用する際のフローチャート



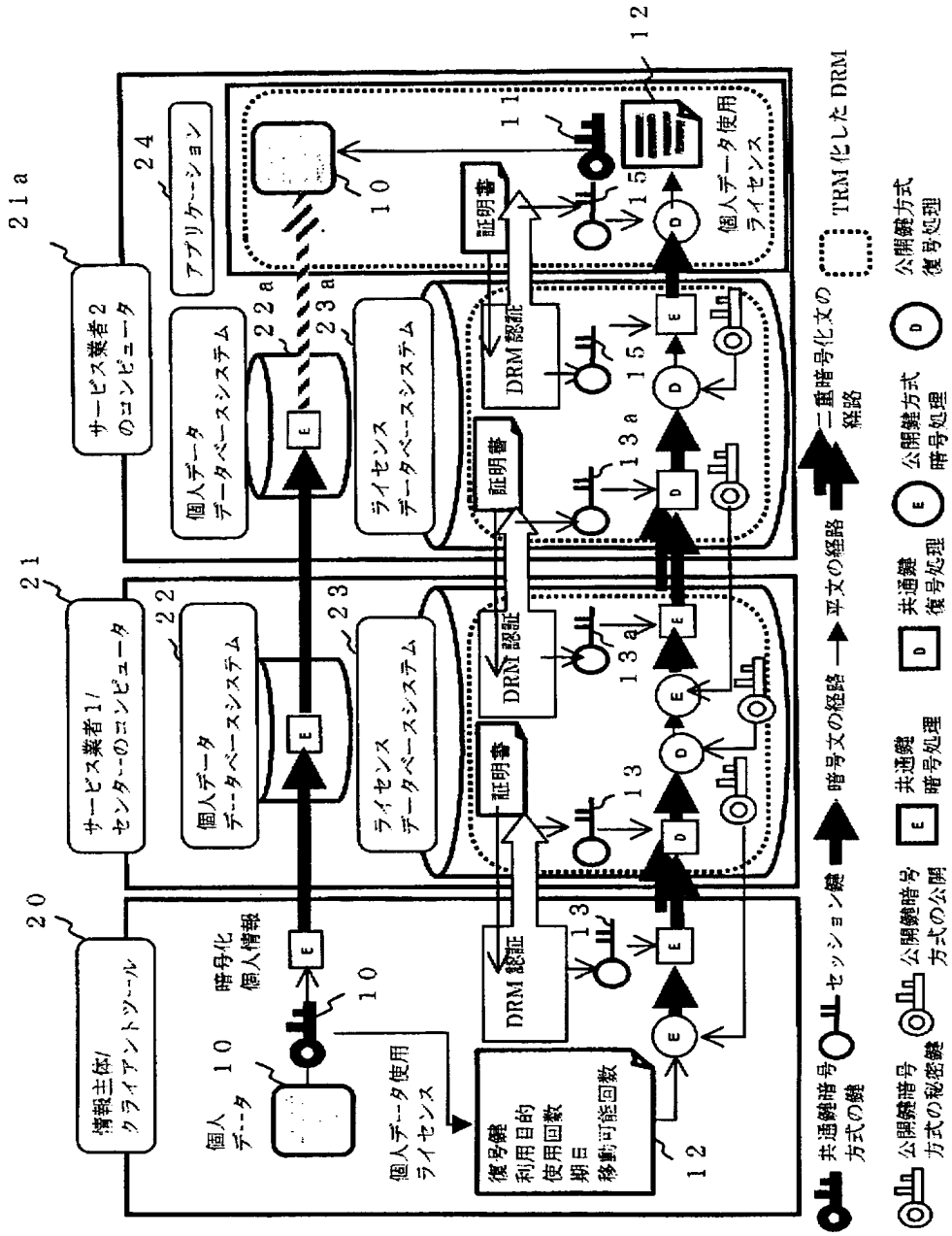
【図９】

ライセンスデータベースシステムの
ライセンス送信時のフローチャート



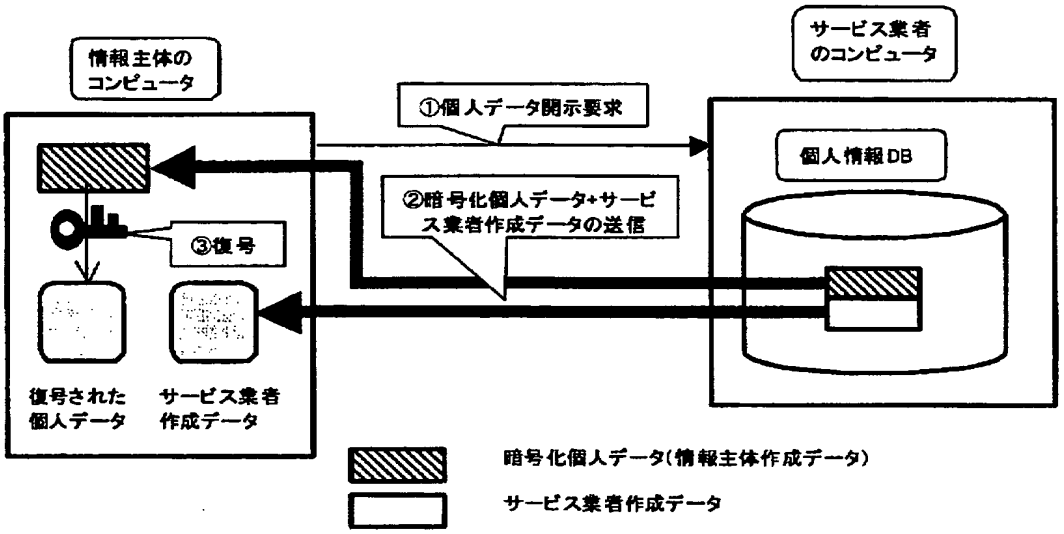
【図１０】

## 本発明の実施形態の別の構成における適用例を説明する図



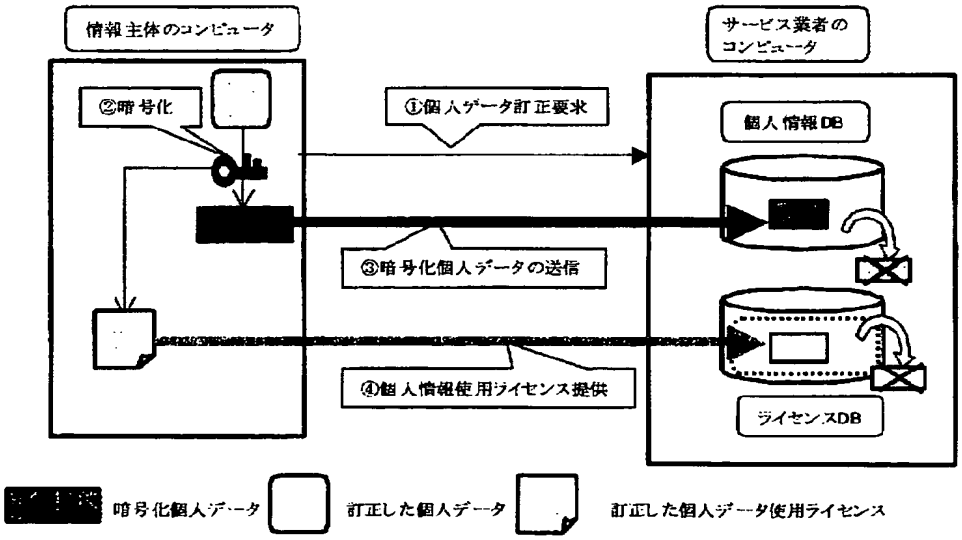
【図１１】

情報主体から開示請求があった場合の開示の仕組みを示す図



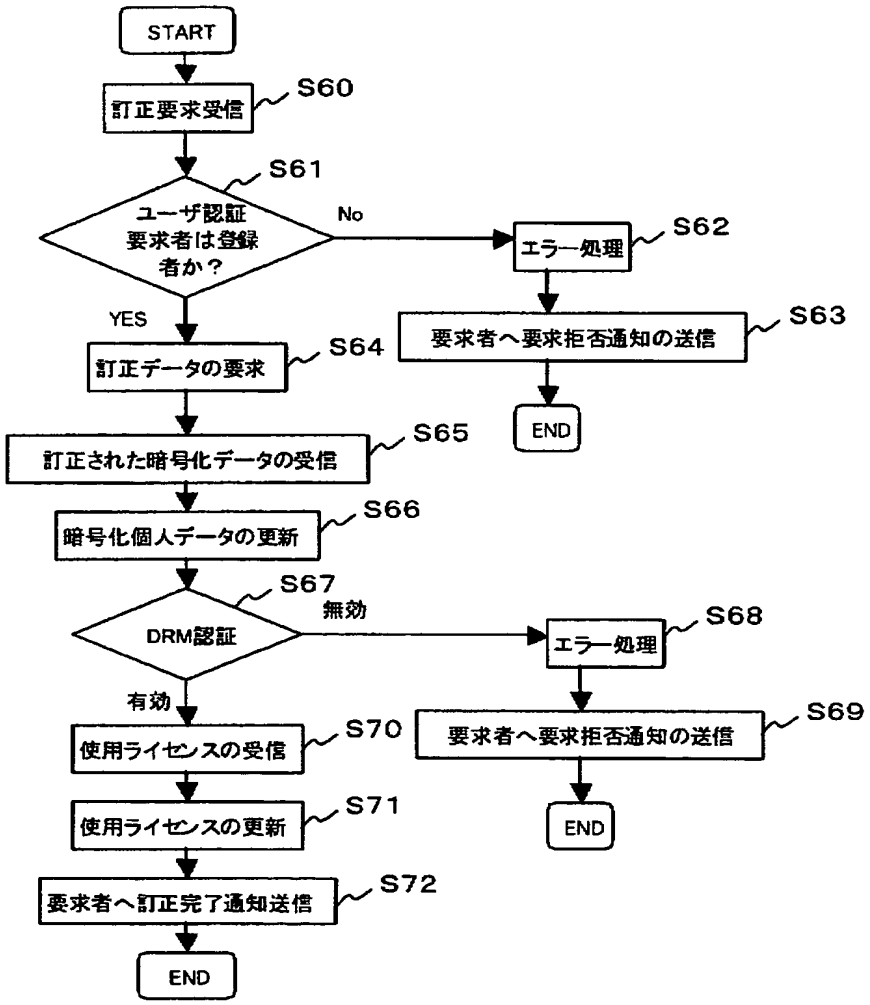

【図１２】

情報主体からの個人データの訂正請求における動作を説明する図



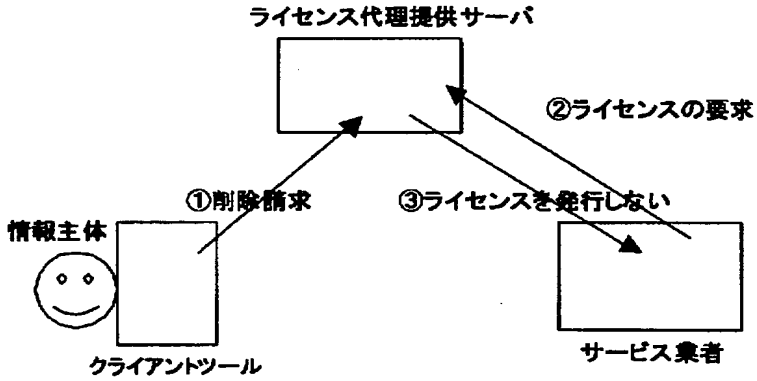
【図１３】

# サービス業者側の個人データの訂正処理のフローチャート



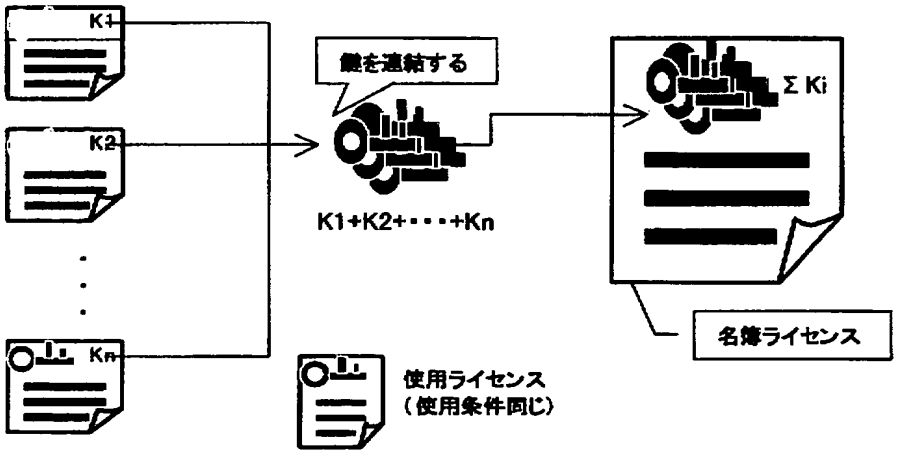
【図１４】

ライセンス代理提供サーバによる
個人データの削除処理を説明する図



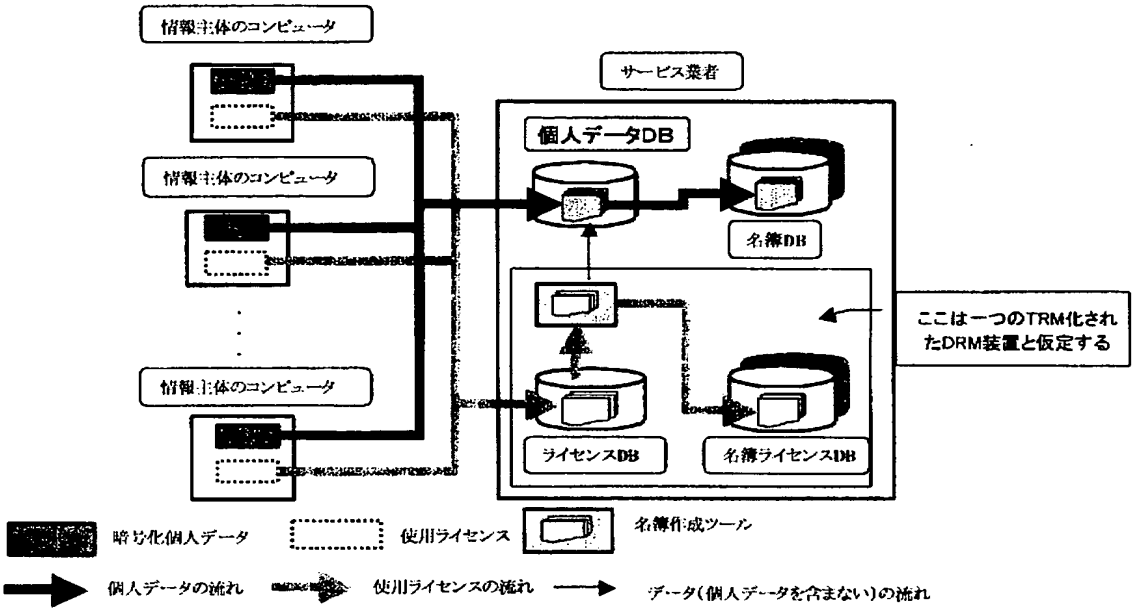

【図１５】

名簿ライセンスの生成処理を説明する図



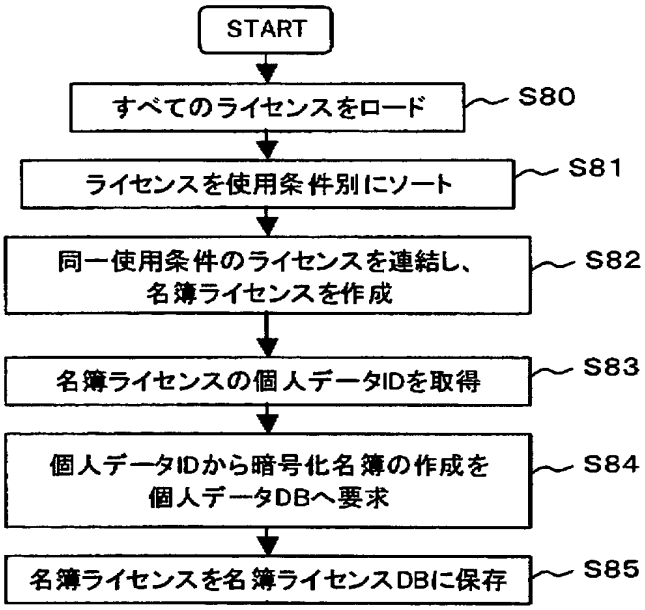
【図１６】

# 名簿の作成と名簿ライセンスの生成処理を図示した模式図



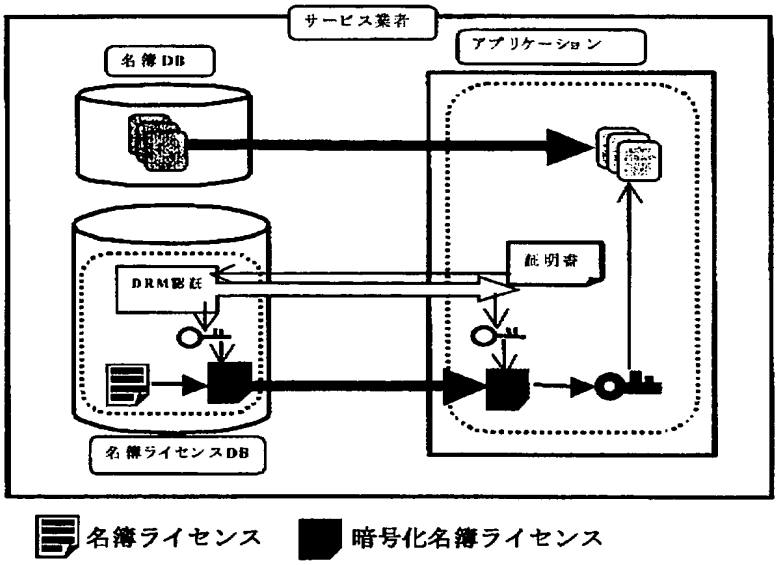
【図１７】

# 名簿作成ツールが名簿・名簿ライセンスを作成する処理のフローチャート



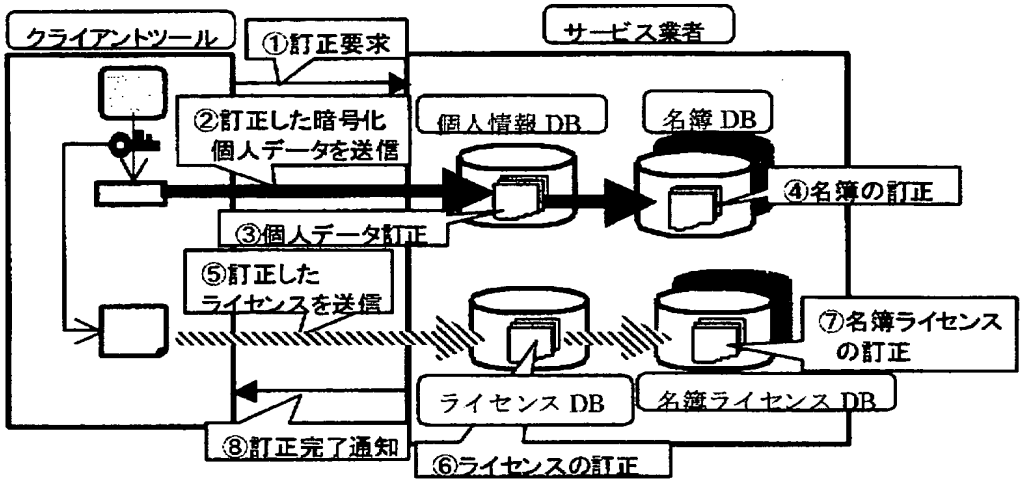
【図１８】

# 名簿の使用形態を説明する図



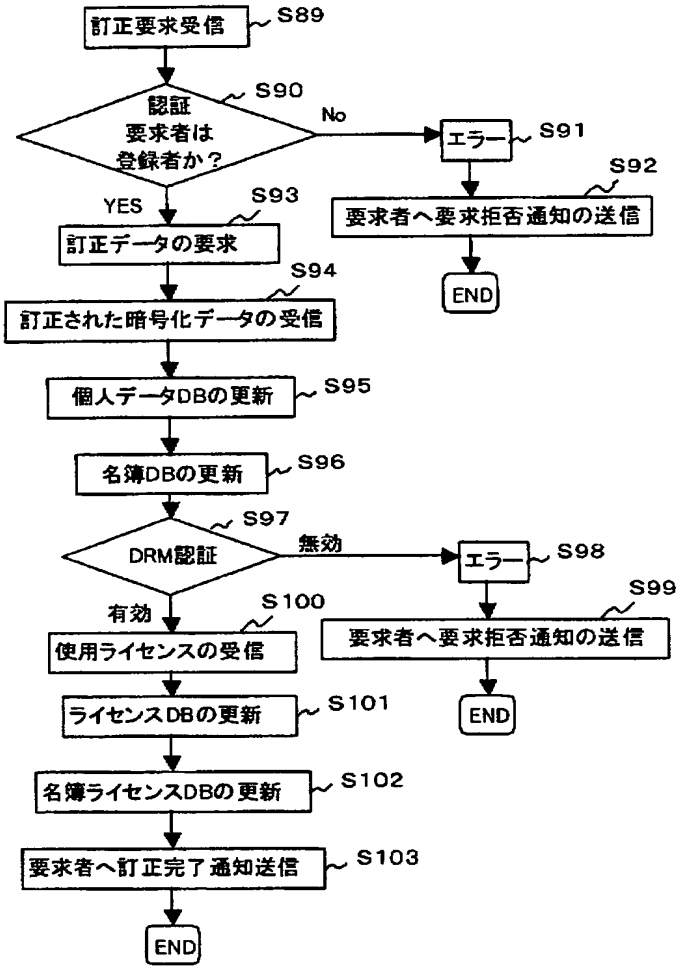
【図１９】

# 名簿使用時の訂正要求の処理を説明する図



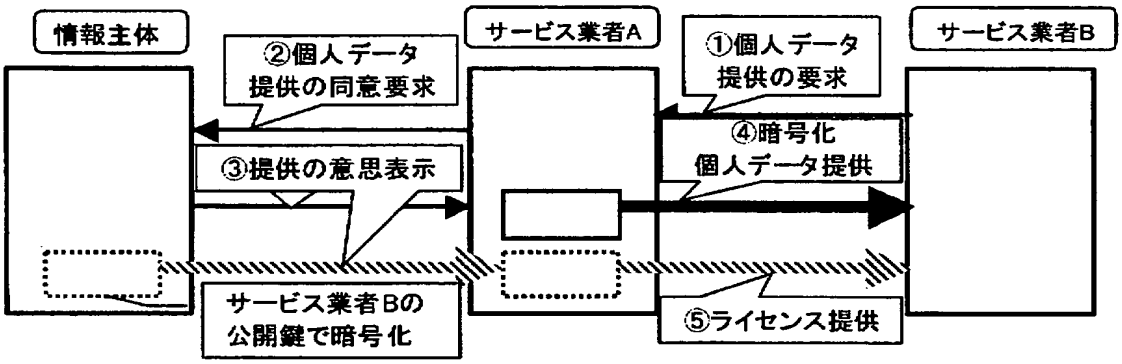
【図２０】

名簿使用時のサービス業者の名簿の訂正処理を示すフローチャート



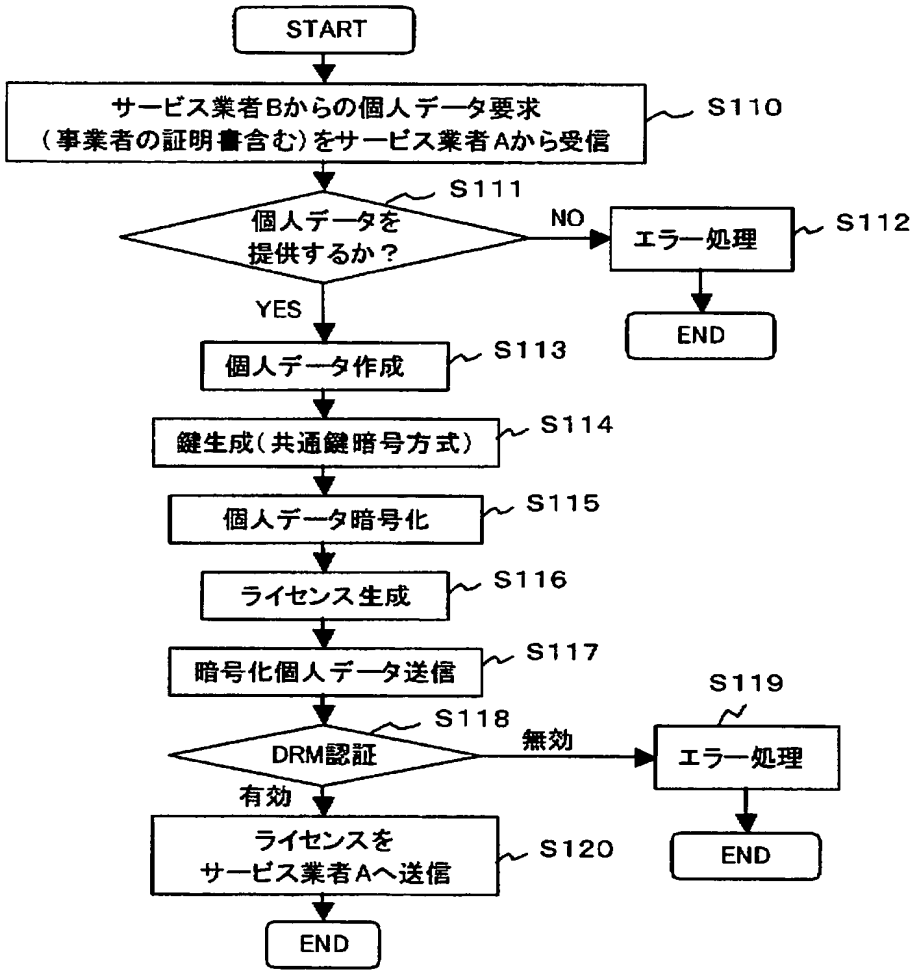
【図２１】

# サービス業者間で個人データを取り引きする処理を示す図



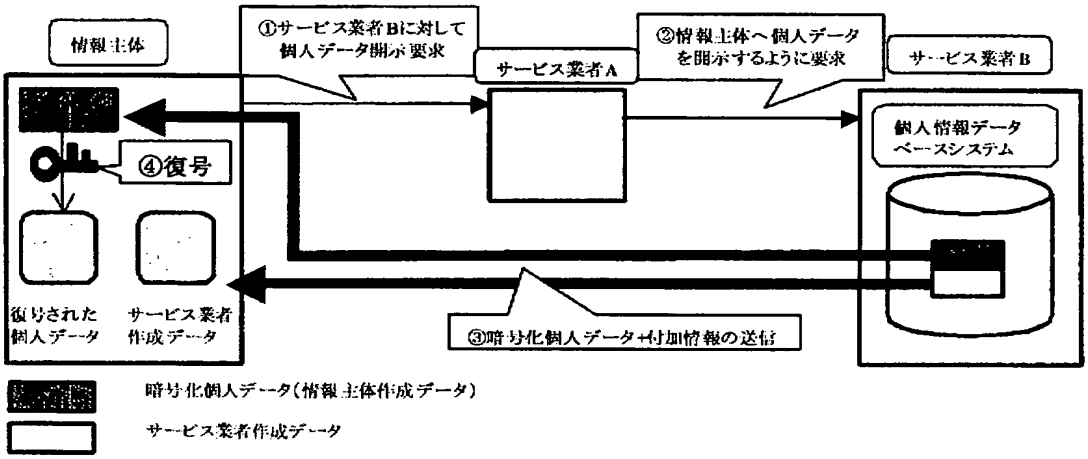
【図２２】

# サービス業者Bへの個人データ使用ライセンスを発行するときのクライアントツールの処理を示すフローチャート



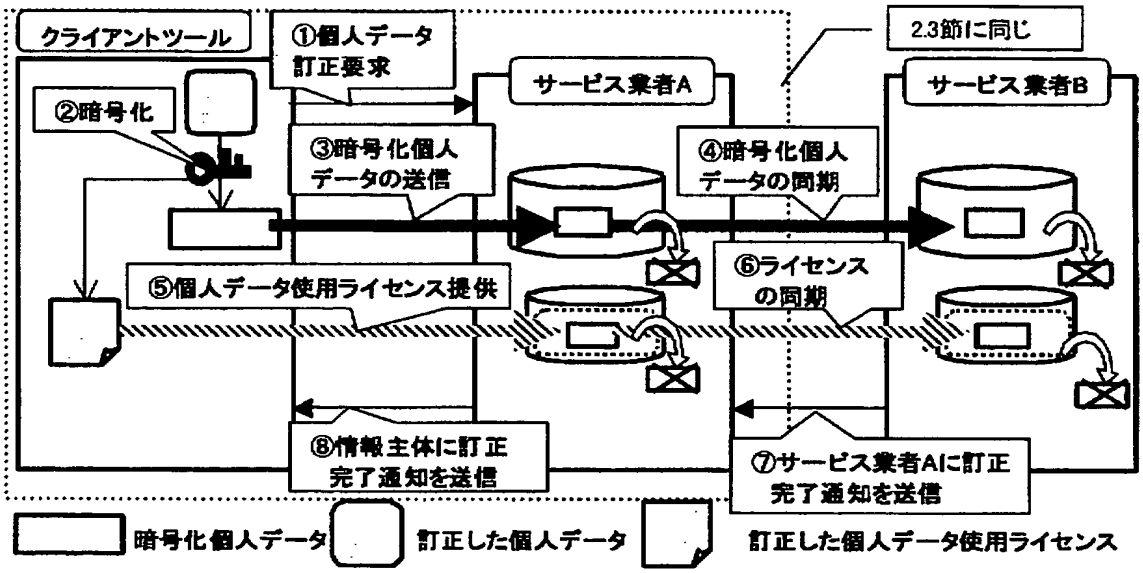
【図２３】

# サービス業者間で個人データを取り引きする場合における、サービス業者Bへの開示請求の処理を説明する図



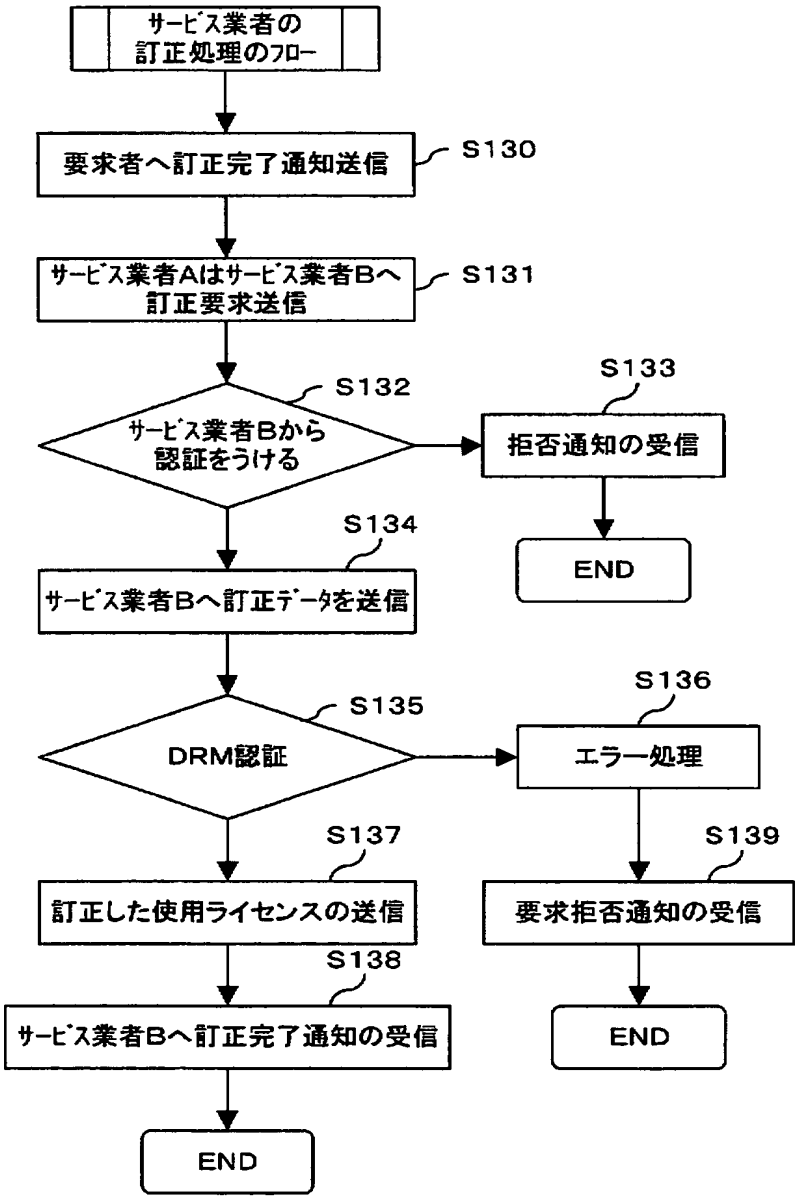
【図２４】

# サービス業者間で個人データを取り引きする場合における訂正請求の処理を説明する図



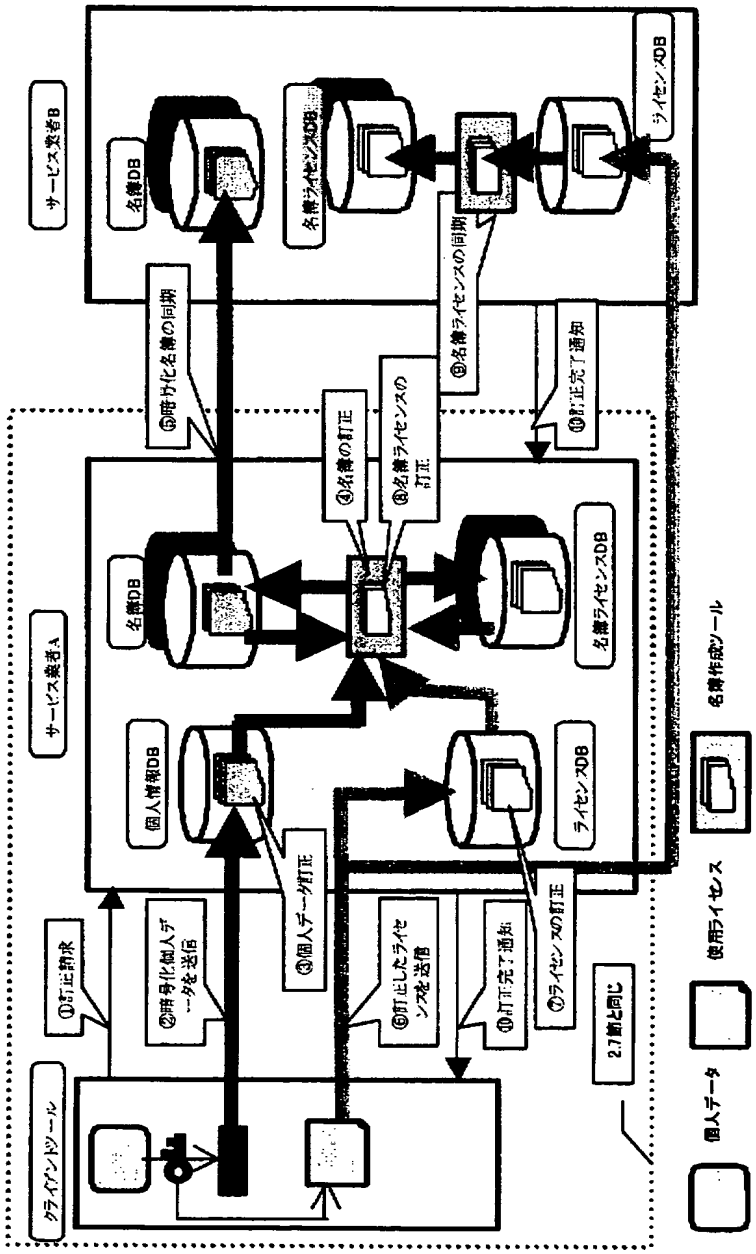
【図２５】

# サービス業者間での個人データの同一性を保つための同期処理を示すフローチャート



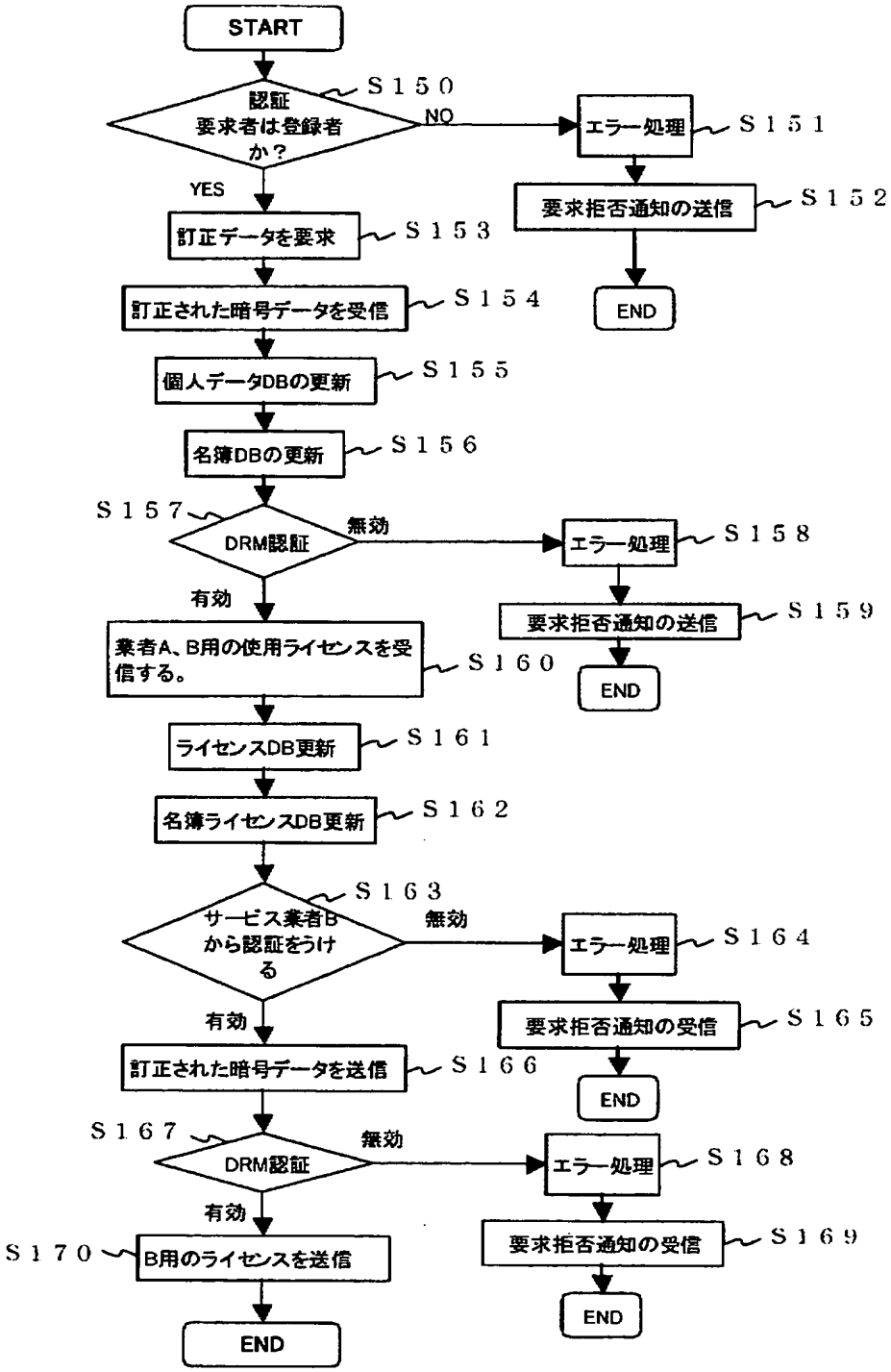
【図２６】

# 名簿を使用する場合の訂正請求の処理を説明する図



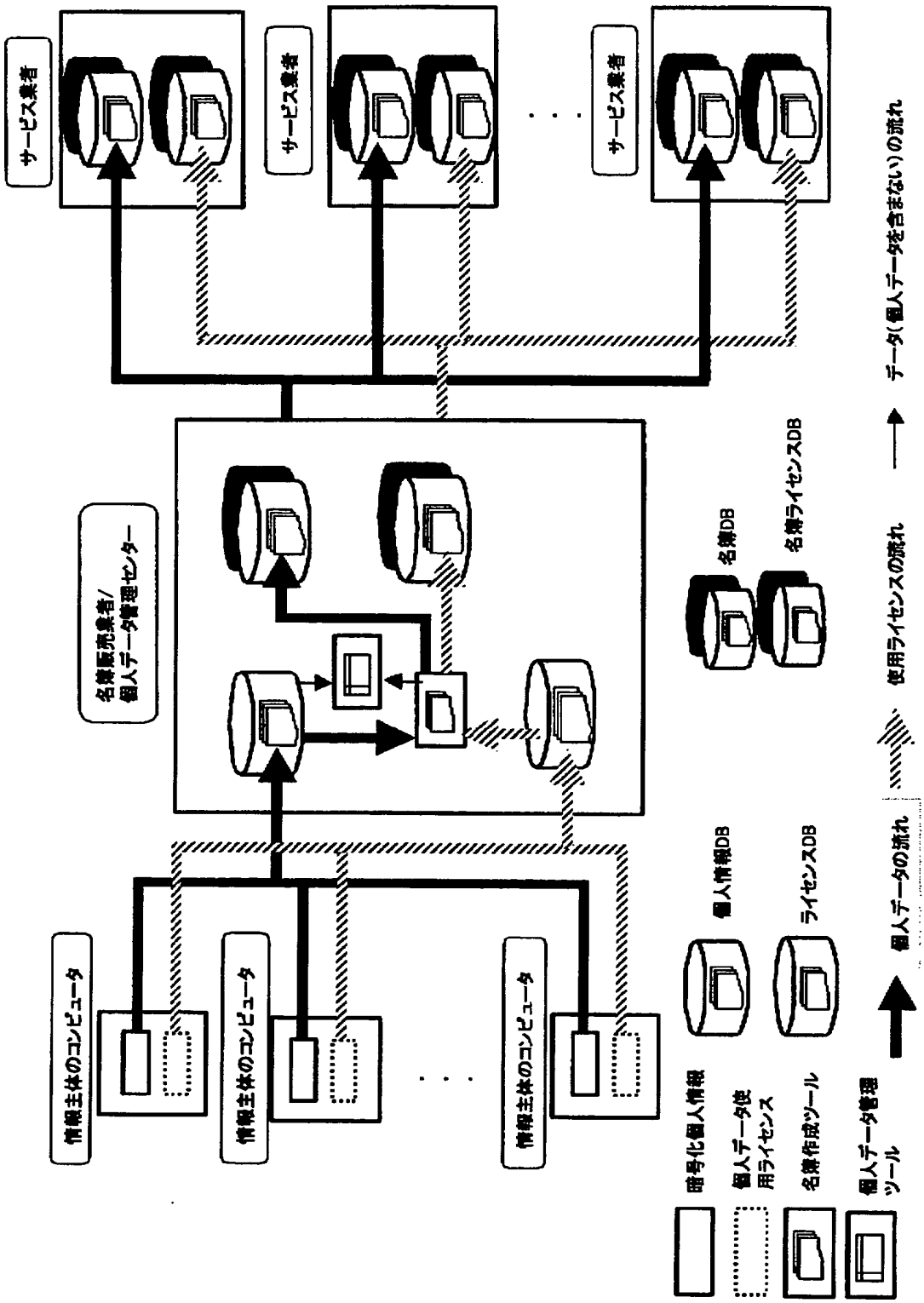
【図２７】

名簿を使用する場合の訂正要求における
サービス業者Aの処理のフローチャート



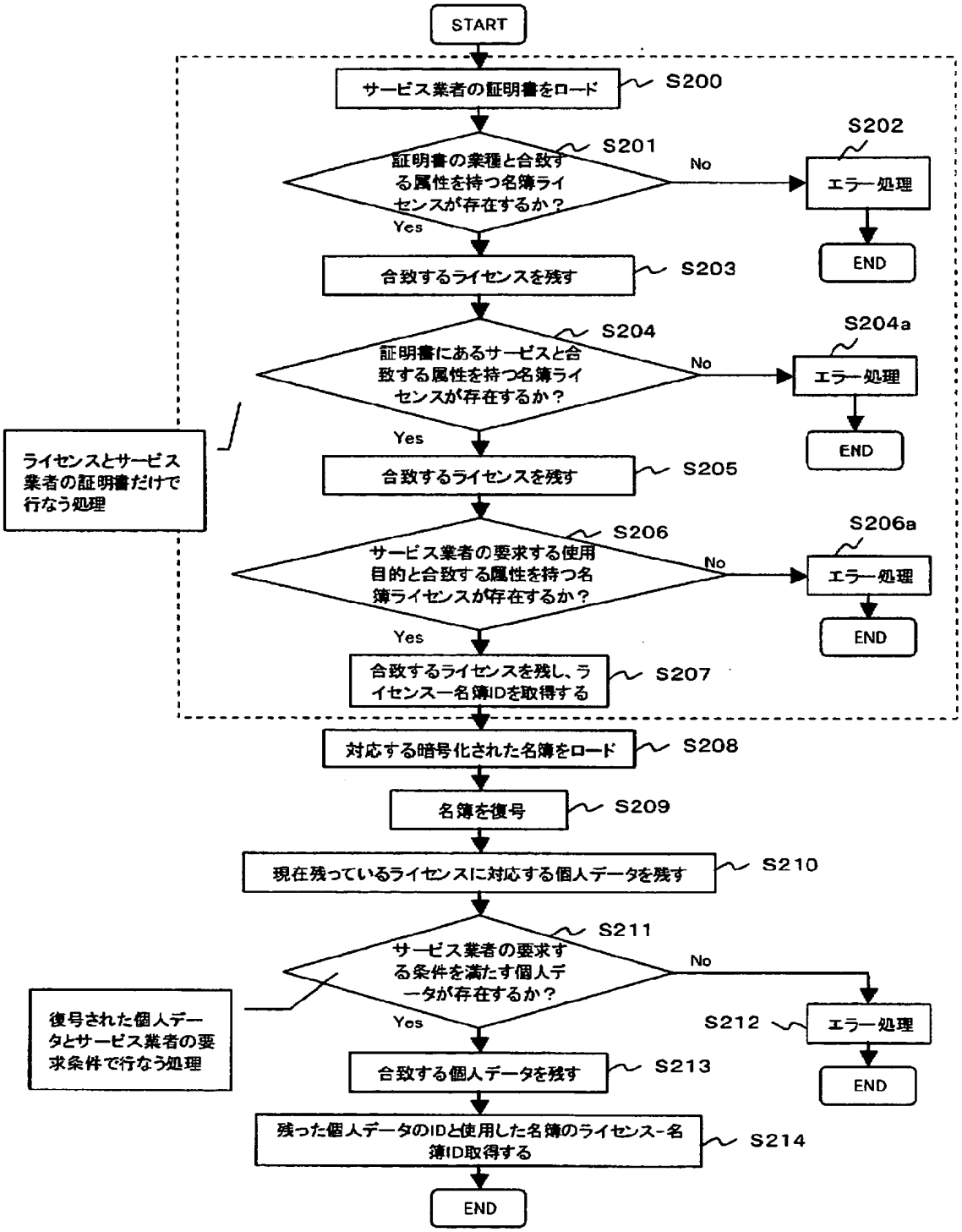
【図２８】

センタ型個人データ提供システムの構成例



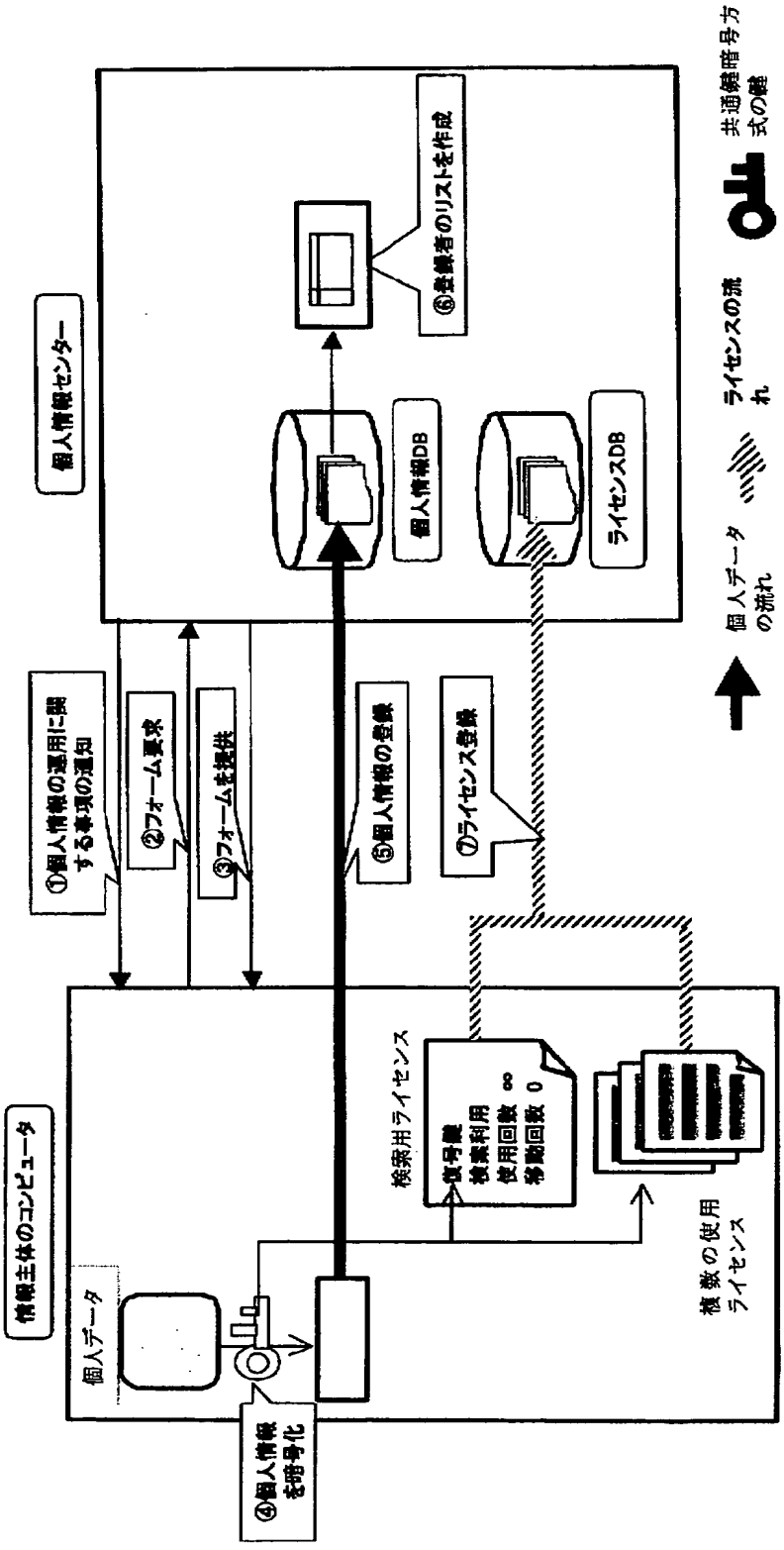
【図２９】

検索ツール処理フローチャートを示す図



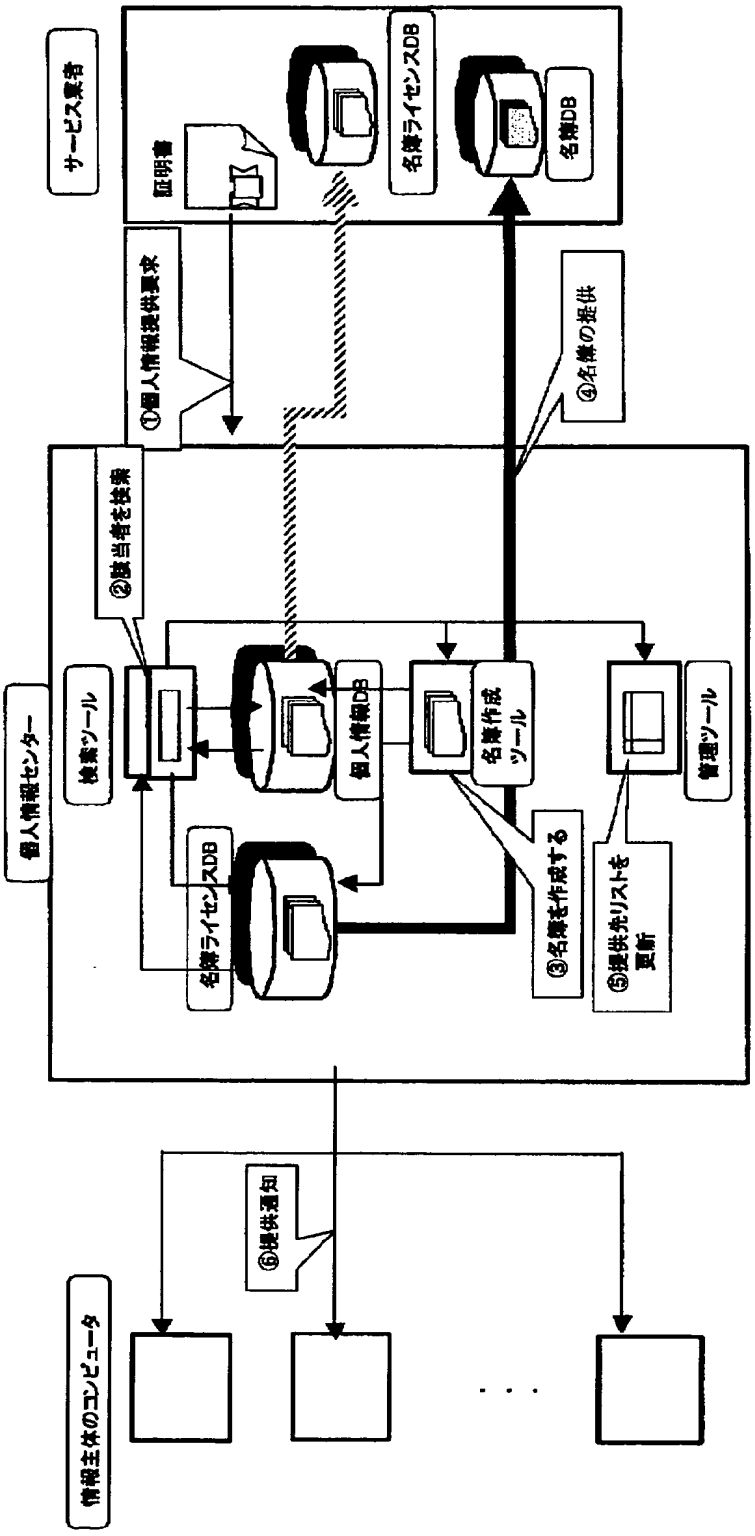
【図３０】

センタへの登録処理を説明する図



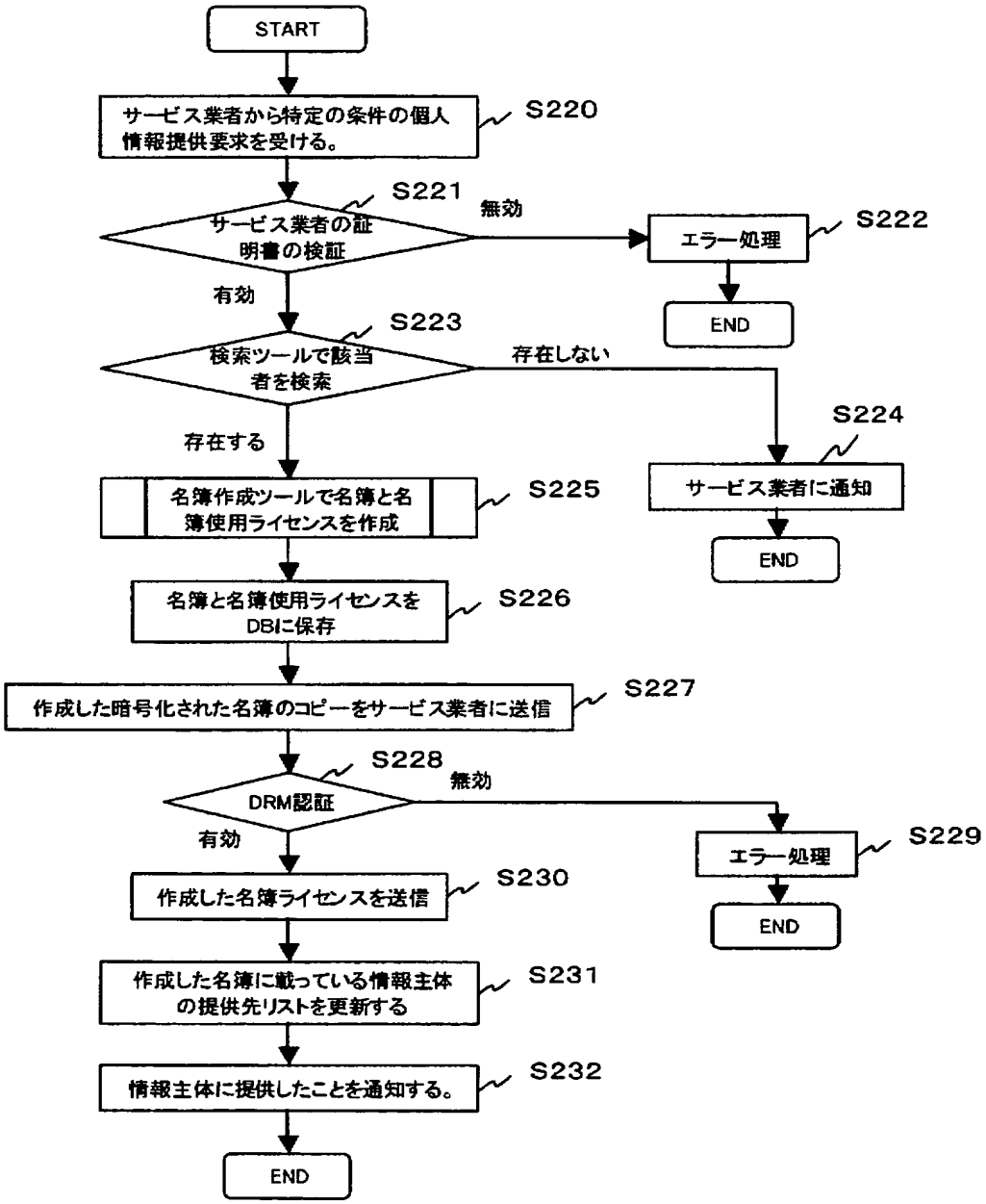
【図３１】

## 個人データの提供処理を説明する図



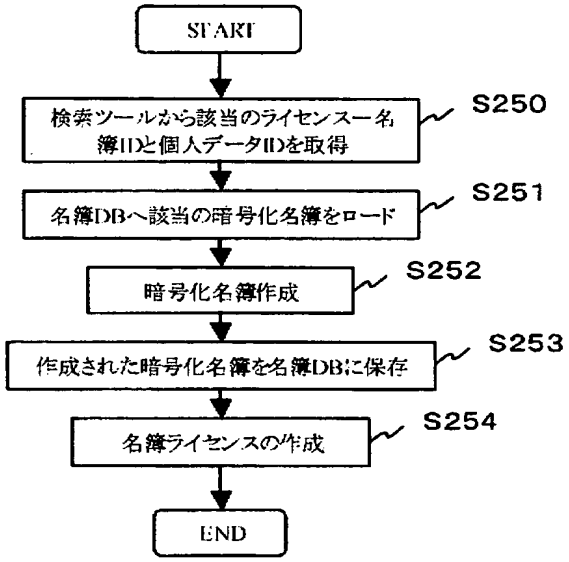
【図３２】

センタの提供処理フローチャート



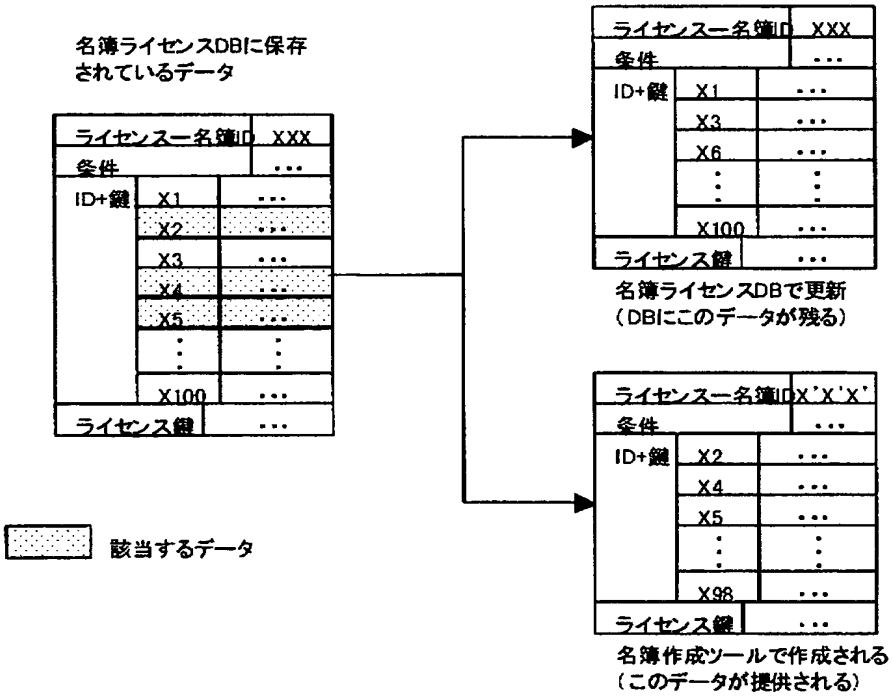
【図３３】

# 名簿作成ツールのフローチャート



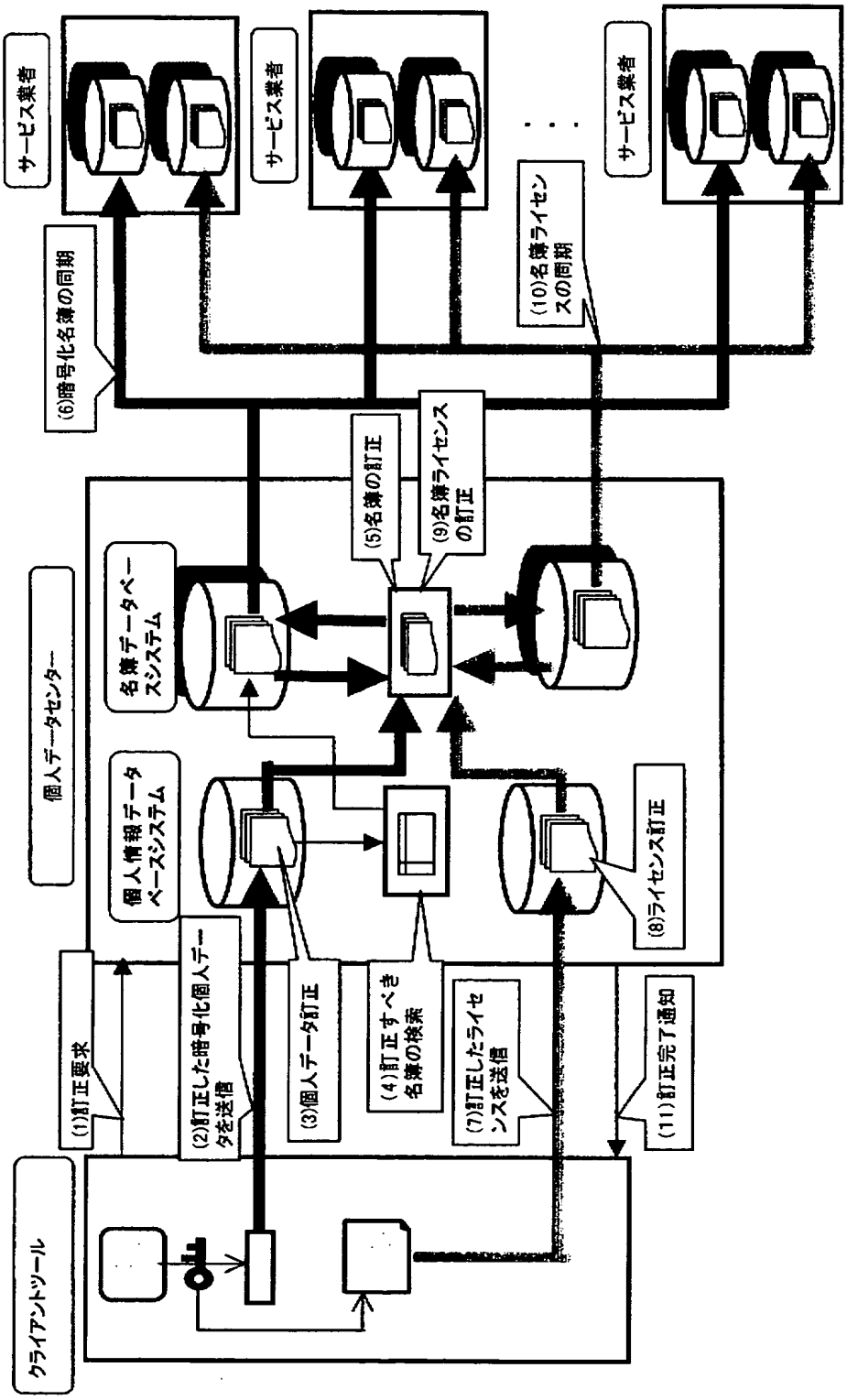
【図３４】

# 提供される名簿ライセンスの作成の概略を示す図



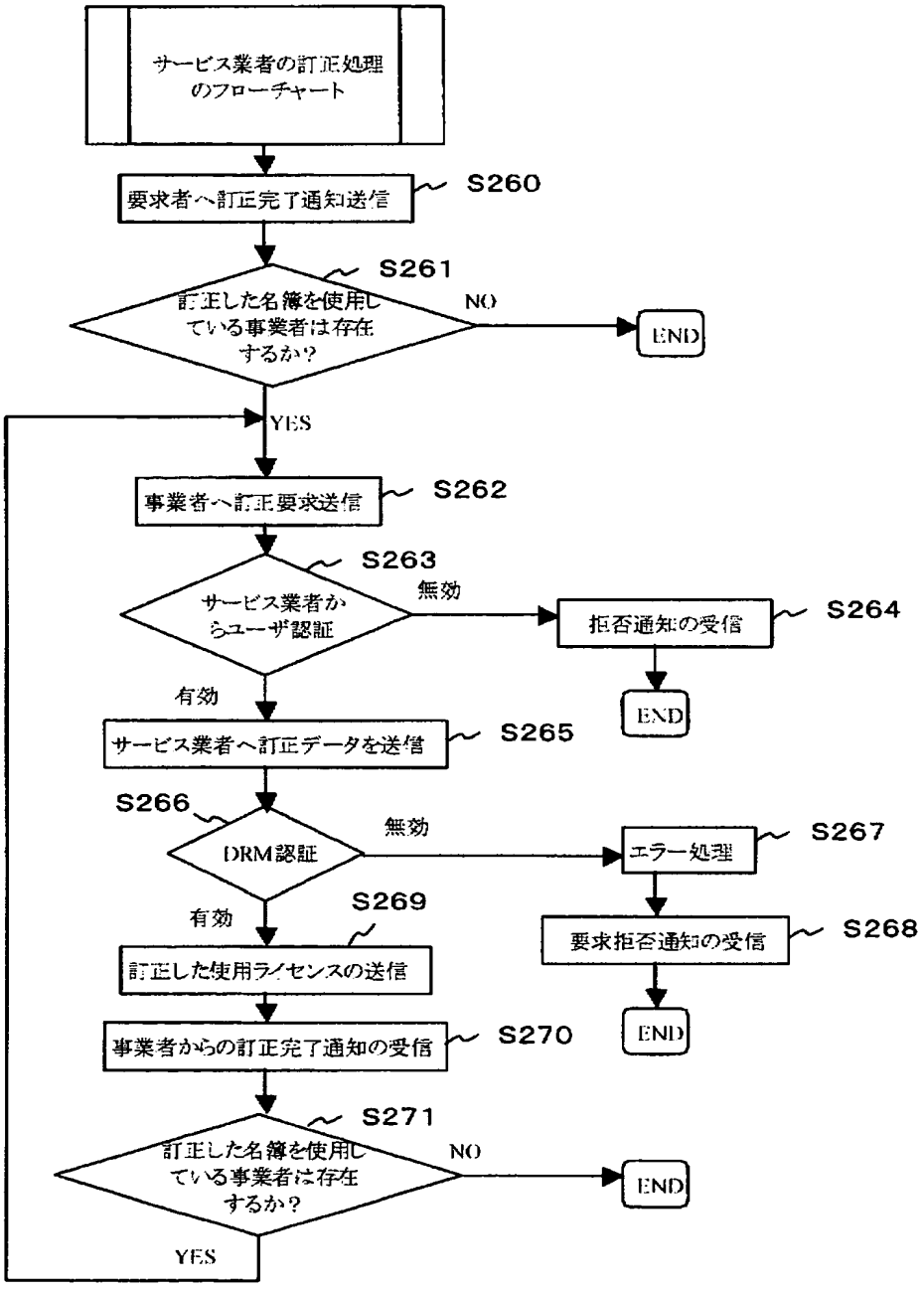
【図３５】

訂正請求の処理の流れを説明した図



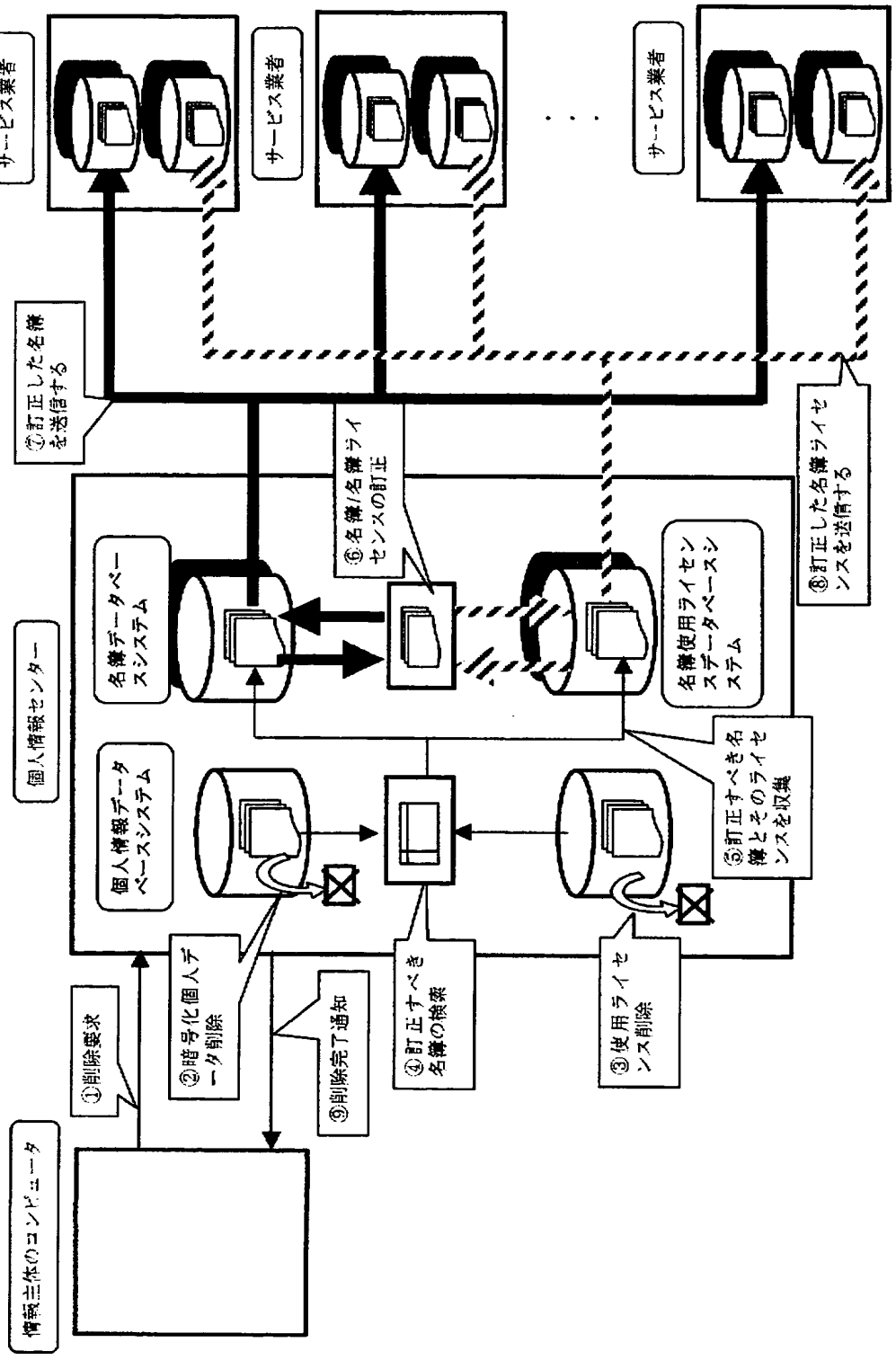
【図３６】

センタの有する個人データの削除処理を説明する図



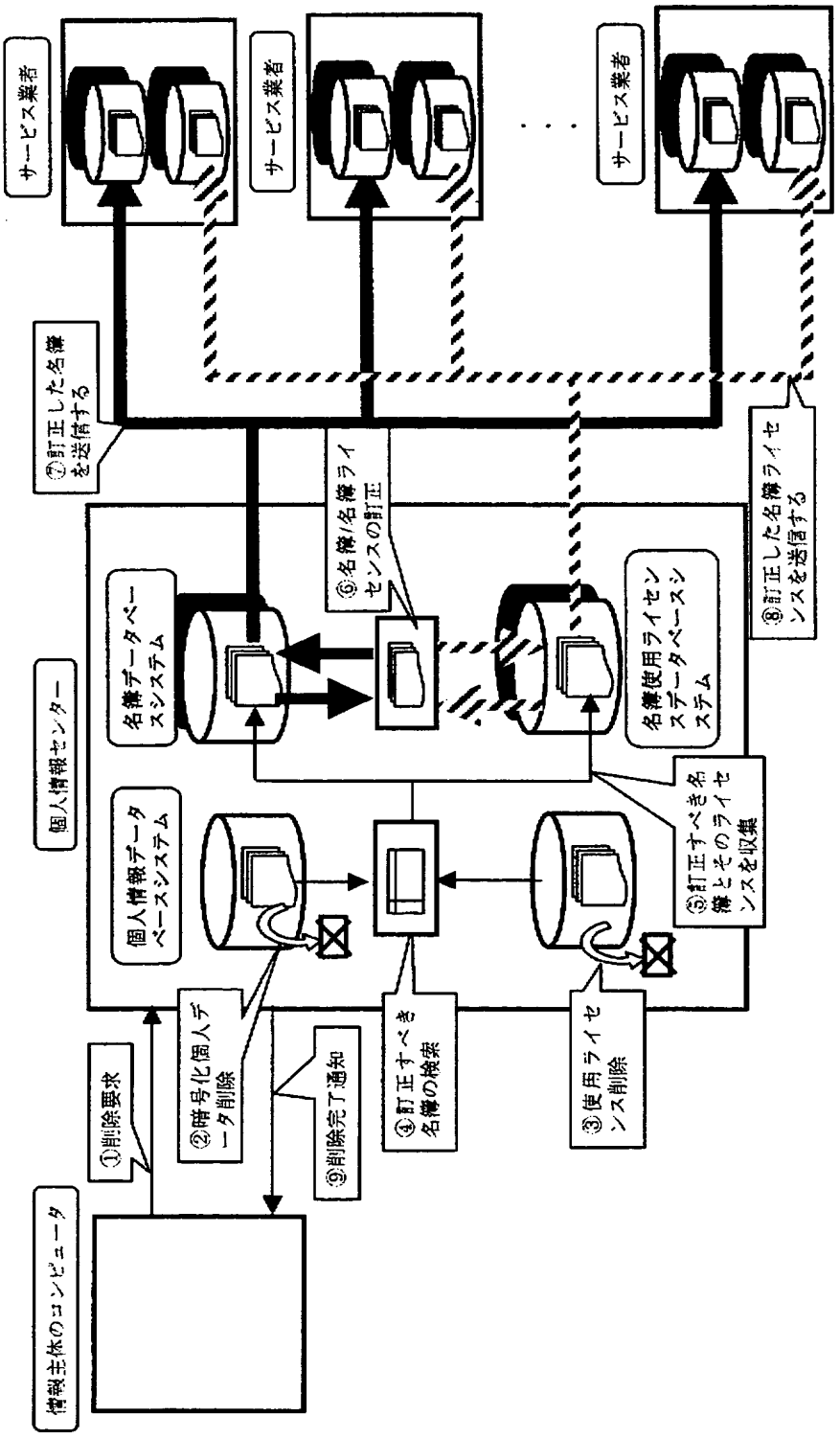
【図３７】

## サービス業者が有する個人データの削除処理を説明する図



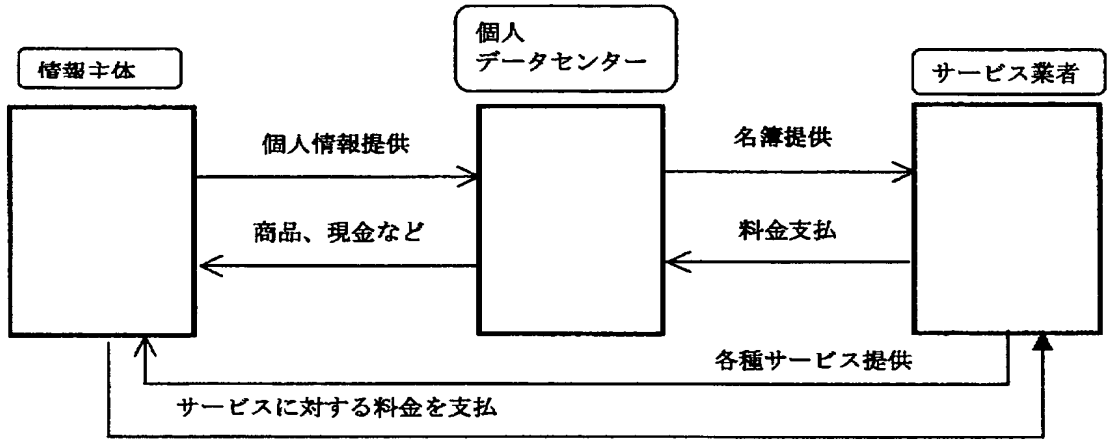
【図３８】

## センタの有する個人データの削除処理を説明する図



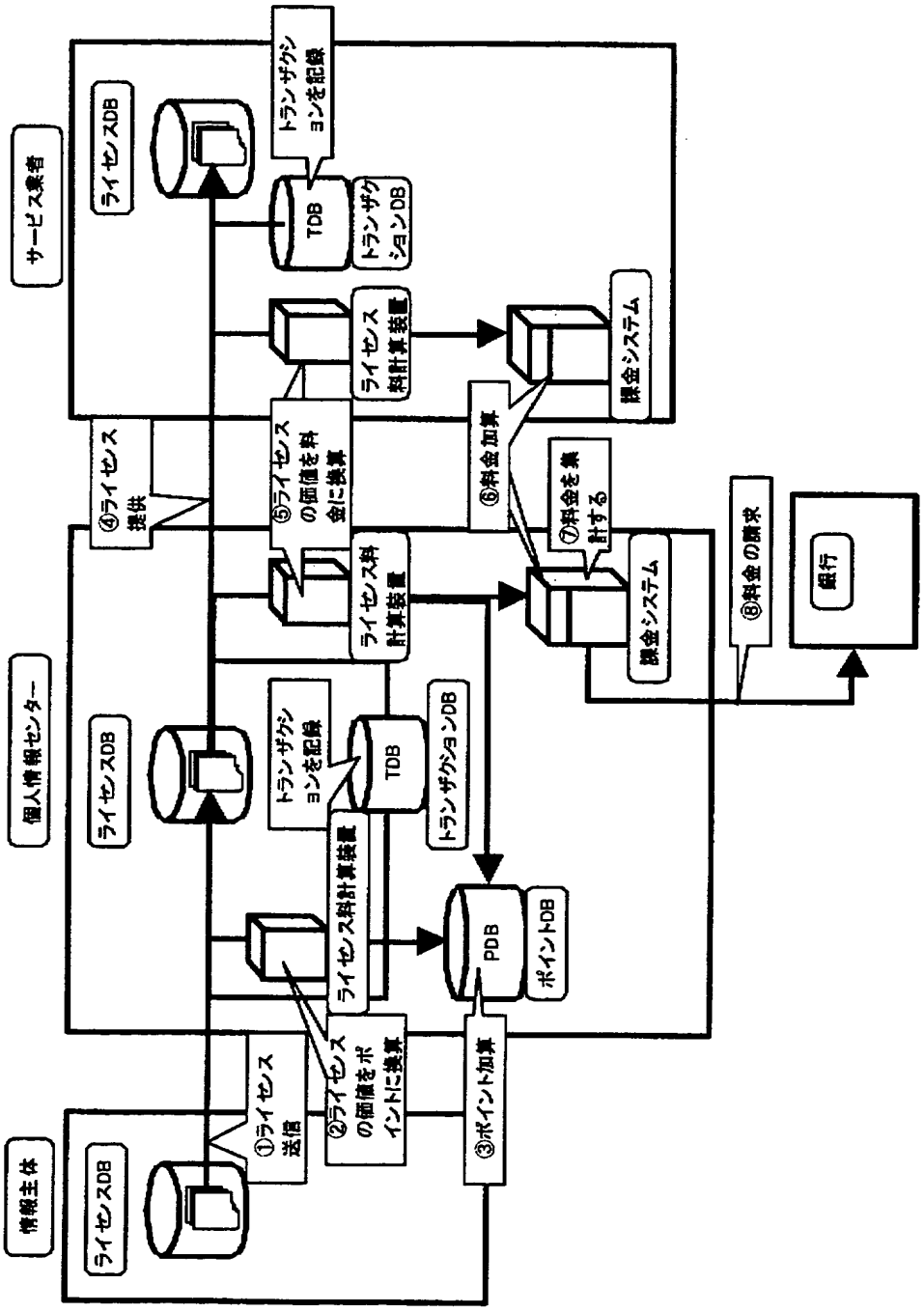
【図３９】

センタ型ビジネスの一形態における情報主体、
センタ、業者の関係を示す図



【図４０】

# データの流れを示す図



【書類名】　　要約書

【要約】

【課題】情報主体の制御の下、個人情報の流通を情報主体の意思に従って制御することができる個人情報保護流通システムを提供する。

【解決手段】情報主体は、クライアントツール２０を使って、個人データの使用を要求するサービス業者のコンピュータ２１に、暗号化された個人データを送る。また、情報主体は、クライアントツール２０を使って、個人データを復号するために使う復号鍵と、利用目的、使用回数、期日、移動可能回数など個人データの利用条件を定めた情報を含めた個人データ使用ライセンスを作成し、ＤＲＭ認証技術を使って、サービス業者のコンピュータ２１に送る。サービス業者は、情報主体が作成した個人データ使用ライセンスに記載された使用条件に合致する場合のみ、個人データを使用することができる。

【選択図】　　図３

特願２００２－２９６７７８

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　　新規登録
住　所　　神奈川県川崎市中原区上小田中１０１５番地
氏　名　　富士通株式会社

２．変更年月日　　１９９６年　３月２６日
［変更理由］　　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社